

CYBER SECURITY ENHANCEMENT ACT OF 2001

HEARING
BEFORE THE
SUBCOMMITTEE ON CRIME
OF THE
COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES
ONE HUNDRED SEVENTH CONGRESS
SECOND SESSION

ON

H.R. 3482

FEBRUARY 12, 2002

Serial No. 58

Printed for the use of the Committee on the Judiciary



Available via the World Wide Web: <http://www.house.gov/judiciary>

U.S. GOVERNMENT PRINTING OFFICE

77-697 PDF

WASHINGTON : 2002

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON THE JUDICIARY

F. JAMES SENSENBRENNER, JR., WISCONSIN, *Chairman*

HENRY J. HYDE, Illinois	JOHN CONYERS, JR., Michigan
GEORGE W. GEKAS, Pennsylvania	BARNEY FRANK, Massachusetts
HOWARD COBLE, North Carolina	HOWARD L. BERMAN, California
LAMAR SMITH, Texas	RICK BOUCHER, Virginia
ELTON GALLEGLY, California	JERROLD NADLER, New York
BOB GOODLATTE, Virginia	ROBERT C. SCOTT, Virginia
ED BRYANT, Tennessee	MELVIN L. WATT, North Carolina
STEVE CHABOT, Ohio	ZOE LOFGREN, California
BOB BARR, Georgia	SHEILA JACKSON LEE, Texas
WILLIAM L. JENKINS, Tennessee	MAXINE WATERS, California
CHRIS CANNON, Utah	MARTIN T. MEEHAN, Massachusetts
LINDSEY O. GRAHAM, South Carolina	WILLIAM D. DELAHUNT, Massachusetts
SPENCER BACHUS, Alabama	ROBERT WEXLER, Florida
JOHN N. HOSTETTLER, Indiana	TAMMY BALDWIN, Wisconsin
MARK GREEN, Wisconsin	ANTHONY D. WEINER, New York
RIC KELLER, Florida	ADAM B. SCHIFF, California
DARRELL E. ISSA, California	
MELISSA A. HART, Pennsylvania	
JEFF FLAKE, Arizona	
MIKE PENCE, Indiana	

PHILIP G. KIKO, *Chief of Staff-General Counsel*

PERRY H. APELBAUM, *Minority Chief Counsel*

SUBCOMMITTEE ON CRIME

LAMAR SMITH, Texas, *Chairman*

MARK GREEN, Wisconsin	ROBERT C. SCOTT, Virginia
HOWARD COBLE, North Carolina	SHEILA JACKSON LEE, Texas
BOB GOODLATTE, Virginia	MARTIN T. MEEHAN, Massachusetts
STEVE CHABOT, Ohio	WILLIAM D. DELAHUNT, Massachusetts
BOB BARR, Georgia	ADAM B. SCHIFF, California
RIC KELLER, Florida	
[VACANCY]	

JAY APPERSON, *Chief Counsel*

SEAN MCLAUGHLIN, *Counsel*

ELIZABETH SOKUL, *Counsel*

KATY CROOKS, *Counsel*

BOBBY VASSAR, *Minority Counsel*

CONTENTS

FEBRUARY 12, 2002

OPENING STATEMENT

	Page
The Honorable Lamar Smith, a Representative in Congress From the State of Texas, and Chairman, Subcommittee on Crime	1
The Honorable Robert C. Scott, a Representative in Congress From the State of Virginia, and Ranking Member, Subcommittee on Crime	2

WITNESSES

Mr. John G. Malcolm, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice	
Oral Testimony	3
Prepared Statement	5
Ms. Susan Kelley Koeppen, Corporate Attorney, Microsoft Corporation	
Oral Testimony	7
Prepared Statement	9
Mr. Clint Smith, Vice President and Chief Network Counsel, WorldCom	
Oral Testimony	13
Prepared Statement	15
Mr. Alan Davidson, Staff Counsel, Center for Democracy and Technology	
Oral Testimony	17
Prepared Statement	19

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

The Honorable Sheila Jackson Lee, a Representative in Congress From the State of Texas	35
The Honorable Bob Goodlatte, a Representative in Congress From the State of Virginia	35
Letter from Mr. Harris N. Miller, President, the Information Technology Association of America (ITAA)	37
Letter from Mr. Doug Lowenstein, President, Interactive Digital Software Association (IDSA), Washington, DC	38
Letter from Mr. Marc Rotenberg, Executive Director, and Mihir Kshirsagar, IPIOP Policy Fellow of the Electronic Privacy Information Center, Washington, DC	39
Letter from Ms. Rachel King and Ms. Katie Corrigan, Legislative Counsel of the American Civil Liberties Union, Washington National Office, Washington, DC	45
Letter from Judge Diana E. Murphy, Chair, United States Sentencing Commission, Washington, DC	48
Letter from Mr. Rhett Dawson, President, Information Technology Industry Council, Washington, DC	51
Statement of Dr. Stephen E. Cross, Director, Software Engineering Institute, Carnegie Mellon University, Pennsylvania, PA	52
News Release from Business Software Alliance, Washington, DC	70

CYBER SECURITY ENHANCEMENT ACT OF 2001

TUESDAY, FEBRUARY 12, 2002

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CRIME,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to call, at 4:05 p.m., in Room 2237, Rayburn House Office Building, Hon. Lamar Smith [Chairman of the Subcommittee] presiding.

Mr. SMITH OF TEXAS. The Subcommittee on Crime will come to order. Now, today we are having a legislative hearing on H.R. 3482, the Cyber Security Enhancement Act of 2001. I will recognize Members for their opening statements after which we will look forward to hearing from the witnesses.

And I will start off by recognizing myself for an opening statement.

Last summer, the Subcommittee on Crime held a series of hearings on cyber security and cyber crime. Since then, mainly after September 11th, much has changed. What has not changed is the increasing need to improve our Nation's cyber security to advance our own technology and to strengthen our criminal laws to prevent, deter and respond to such attacks.

As we increase individual's physical safety at our airports, borders and even sporting events, we should not forget to strengthen cyber security as well. Just as a physical attack could cause destruction, a cyber attack could substantially harm our economy and endanger public health and lives.

This hearing affords the Subcommittee an opportunity to review H.R. 3482, the Cyber Security Enhancement Act of 2001, which includes law enforcement technology and strengthens criminal laws.

Last summer's hearings highlighted the growing threat of cyber crime and cyber terrorism against our citizens and our Nation. Criminals, whether they are terrorists or vandals, use computers and other types of technology to threaten lives, incomes, businesses and our Nation's future. At the previous hearings, law enforcement officials testified that better training, additional resources and increased cooperation and coordination are needed. Private industry testified that cyber crime was a growing problem and cost businesses and the economy billions of dollars every year. Those witnesses urged the Subcommittee to strengthen the penalties for such attacks and improve the coordination and information-sharing capabilities of law enforcement agencies and businesses.

In response to those hearings, I drafted the Public Safety and Cyber Security Enhancement Act of 2001. Most of H.R. 2915 was adopted as part of the USA Patriot Act, the antiterrorism bill that was enacted in October 2001. To address the issues that were not incorporated, as well as new ones, we introduced a bill that we have before us today.

This legislation increases penalties to better reflect the seriousness of cyber crime, enhance the Federal, State and local law enforcement efforts through better coordination, and assist State and local law enforcement through better grant management, accountability and dissemination of technical advice and information. Additionally, the bill helps protect the Nation's critical infrastructure by authorizing and supporting the National Infrastructure Protection Center, which handles threat assessment and responds to attacks on the Nation's critical infrastructure from both physical and cyber sources.

America must protect our national security, critical infrastructure and economic base from attack, including the growing threat of cyber attacks. Penalties and law enforcement capabilities must be adequate to prevent and deter such attacks.

The chairman of the board, Bill Gates—or I should say chairman of the board of Microsoft, Bill Gates, recently declared that making Microsoft's software less vulnerable to security breaches would take precedent over adding new features, and Oracle's chief security officer said, "one of the most threatening types of attack is one that is launched in cyberspace to bring down our critical infrastructures." And Richard Clark, the White House cyberspace security adviser stated, "there is a willingness to admit that there are vulnerabilities, and it is not inconceivable that they will be used against us in a way that could be very damaging to our economy."

So bolstering our homeland defense, while neglecting cyber security, is like locking the front door of your house but leaving the windows wide open. As a matter of national and economic security, we cannot afford to let technology be our weakest link. With that goal in mind, we welcome our witnesses today and look forward to their comments on this legislation that we have before us. I will now recognize the Ranking Member, Bobby Scott, for his opening statement.

Mr. SCOTT. Thank you, Mr. Chairman, and I appreciate your holding this hearing on H.R. 3482, the Cyber Security Enhancement Act of 2001. I also appreciate the studious approach in which you have approached the issue of cyber crime in general. And by taking this approach, you can make sure that we are doing substantively the best job that we can do. This is our fourth hearing on the issue over the past year in which we have looked at the Federal effort and responsibility, the State and local effort and responsibility and the effort and responsibility of the private sector.

One of the things we have learned is that we risk overreacting to the threats with a heavy-handed law enforcement approach. Indeed, in the USA Patriot Act, we actually repealed some approaches which were found to be virtually unenforceable because they were so heavy-handed. Indeed, we have worked with the industry to give it a chance to develop stronger security systems, and I believe that approach has worked well.

So, Mr. Chairman, I am pleased to see that in the bill before us, of which you are the chief sponsor, there is no such heavy-handed law enforcement approaches. There are some sensible enhancements in the bill, and we may want to make sure that we are doing—that what we are doing does not conflict with the work of the Sentencing Commission already in this area.

I am sure we can work those issues out. The primary concern I have with the bill is in section 102, which expands the emergency sharing of private information with law enforcement to address threats of death and serious injury. We approved this in the Patriot Act. However, the bill changes the showing required for release of such information from reasonable cause to good faith. As you will recall, Mr. Chairman, during the consideration of the issue in the Patriot Act, a number of us fought the relaxation of the traditional probable cause standard for access to private information by law enforcement and voted for only reluctantly as a compromise on the bill as a whole.

Although the Senate amendments tighten the process some, many of us have remained uneasy with the reasonable cause standard. Now we are faced with further loosening of the standard, and I am not convinced that the case has been made for that yet.

I understand the Department of Justice has concerns with the organizational changes called for in the bill, and we want to hear more from them before we reach conclusions. So I look forward to the testimony of the witnesses to shed light on these matters and look forward with working with you to address the issues in the legislation—as the legislation moves forward.

Thank you, Mr. Chairman.

Mr. SMITH OF TEXAS. Thank you, Mr. Scott, for your comments, and I am hopeful that our witnesses today will address some of the questions that you have raised as well.

Does the gentleman from North Carolina, Mr. Coble, whom we are glad to see, have an opening statement?

Mr. COBLE. No opening statement, Mr. Chairman. Thank you.

Mr. SMITH OF TEXAS. Thank you, Mr. Coble. Let me proceed now. I will introduce our witnesses, as I say, to hear from them directly. Our witnesses are John G. Malcolm, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice; Susan Kelley Koeppen, former prosecutor with the Department of Justice, I might add, who is now the corporate attorney for Microsoft Corporation; Clint Smith, Vice President and Chief Network Counsel of WorldCom; and Alan Davidson, Staff Counsel, Center for Democracy and Technology.

Mr. SMITH OF TEXAS. Now, we welcome you all. Obviously, we look forward to your testimony, and Mr. Malcolm, we will begin with you.

STATEMENT OF JOHN G. MALCOLM, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE

Mr. MALCOLM. Thank you, Mr. Chairman. Mr. Chairman, and Members of the Subcommittee, thank you for giving me this opportunity to testify on behalf of the criminal division of the Department of Justice regarding title I of H.R. 3482, the Cyber Security

Enhancement Act of 2001. Mr. Chairman, I commend you for sponsoring a bill addressing the issue of computer crime, an issue that is of the utmost importance to our national defense and security, to the strength and vitality of our economy and to the health, safety and privacy of our citizens.

Internet crime is on the rise. A recent Washington Post article reported that one Internet security firm documented more than 128,000 unauthorized accesses to its clients' computer systems between July and December of last year alone. The Computer Security Institute estimates that the economic loss resulting from such crimes has more than doubled in the last 5 years, and America's ongoing war on terrorism casts such crimes in a grave new light.

Title I of H.R. 3482 increases penalties, thereby deterring more effectively those who would commit computer crimes. The Department strongly supports title I. The Department recommends, however, that the Subcommittee consider two changes: First, the Department urges the Committee to consider broadening slightly the scope of section 106 so that it covers not only hackers who damage computer systems knowing that death or serious injury will result, but also hackers who actually cause death or serious injury by damaging a computer system with reckless disregard for these outcomes.

In an era in which computer systems play an integral role in our critical infrastructures, such as electrical power, telecommunications and medical care, the law should clearly warn would-be hackers of the potential consequences of their actions and hold them fully responsible if they recklessly disregard those consequences.

Consider, for example, a hacker who shuts down a town's phone service. While phone technicians race frantically to restore service, no emergency 9-1-1 calls can go through. As a result, several people needing urgent medical care may die or be seriously injured. Although the hacker might not have known that his conduct would cause death or serious bodily injury, such reckless conduct may well merit punishment greater than the 10 years currently provided by the statute.

Mr. Chairman, the Internet is a powerful tool, but when the Internet is misused by criminals, it is turned into a harmful weapon. When criminals intentionally damage computer systems recklessly causing severe harm or even death to others, they must be held fully responsible. Thus, the Department encourages this Subcommittee to expand the scope of section 106 to include criminals who recklessly cause death or serious bodily injury.

Second, the Department encourages the Committee to modify section 101 so that it more clearly directs the Sentencing Commission to enhance penalties as you are reexamining the sentencing guidelines that pertain to computer crimes. In my written testimony, which has been provided to the Committee and which I would like to be made a part of the record, I have set forth three suggestions to better achieve this result. With the help of the Chairman and of this Subcommittee, Congress has made great strides to modernize the laws that relate to the investigation and prosecution of cyber crime. We at the Department of Justice look

forward to continuing to work with this Committee to address new issues as they arise in this evolving area of law.

Mr. Chairman, that concludes my prepared remarks. I would like to thank you and the Subcommittee again for soliciting the views of the Department of Justice on these important issues, and for allowing me to express them through my oral presentation today. I would be happy, of course, to answer any questions the Subcommittee may have.

Mr. SMITH OF TEXAS. Okay. Thank you, Mr. Malcolm, and I will say to you as I would say to all witnesses that your entire testimony will be made a part of the record. Without objection. But we appreciate also your keeping your testimony within 5 minutes, which you have done very well. Thank you, Mr. Malcolm.

[The prepared statement of Mr. Malcolm follows:]

PREPARED STATEMENT OF JOHN G. MALCOLM

Mr. Chairman and Members of the Subcommittee, thank you for giving me this opportunity to testify on behalf of the Criminal Division of the Department of Justice regarding Title I of H.R. 3482, the Cyber Security Enhancement Act of 2001. Mr. Chairman, I commend you for sponsoring a bill addressing the issue of computer crime, an issue that is of the utmost importance to our national defense and security, to the strength and vitality of our economy, to the health and safety of our citizens, and to the privacy of every individual.

Working with our partners in state and federal law enforcement, the Department of Justice has made great strides in recent years in investigating and prosecuting computer crime. Through the Department's Computer Crime and Intellectual Property Section, we have trained scores of federal prosecutors and developed a strong network of computer crime coordinators that extends to every United States Attorney's office. We have expanded the Computer Crime and Intellectual Property Section and have established Computer Hacking and Intellectual Property units in key districts. Not only have these prosecutors addressed computer hacking violations and intellectual property theft, but they have provided expertise critical to the ongoing terrorism investigation.

Despite these important achievements, Internet crimes are on the rise. A recent Washington Post article reported that one Internet security firm documented more than 128,000 unauthorized accesses to its clients' systems between July and December last year. The Computer Security Institute estimates that the economic loss resulting from such crimes has more than doubled in the last five years. These crimes also pose a grave threat to the security, safety, and privacy of all Americans. Just last year, federal law enforcement officers captured two Russian hackers who had infiltrated American banks and businesses, stolen private data, including credit card numbers, and extorted those companies by threatening to destroy their computers or release their customers' private information. Had these criminals not been apprehended, the damage they could have done to credit card holders would have been difficult to overstate.

Title I of H.R. 3482 strengthens the deterrent effect of current laws by increasing penalties and closing loopholes. The Department strongly supports these amendments. The Department recommends, however, that the Subcommittee consider three changes to Title I. The first change would modify section 106 to address the increasing threat of death or serious bodily injury that computer hackers might *recklessly* cause. The second change would provide a more structured mandate to the Sentencing Commission, directing it to tailor the Sentencing Guidelines to address the burgeoning problem of computer crime in the United States. These two suggested changes are addressed in greater detail below.

The third suggested change concerns section 104(a) of the bill. This provision directs the Attorney General, "acting through the Federal Bureau of Investigation, to establish and maintain the National Infrastructure Protection Center to serve as a national focal point for threat assessment, warning, investigation and response attacks on the Nation's critical infrastructure for physical and cyber sources. The Administration requests that the phrase, 'acting through the Federal Bureau of Investigation,' be stricken from section 104(a). As a matter of efficiency and effectiveness in government and good drafting practice, statutes that grant authority to the Attorney General should not limit which of his subordinate officers or organizations in the Department of Justice he can act through.

I. PUNISHMENT OF CRIMINALS WHO RECKLESSLY CAUSE DEATH OR SERIOUS BODILY INJURY THROUGH COMPUTER HACKING

Section 106 institutes a welcome increase in the penalty for crimes committed in the cyber world when the criminal *knows* that death or serious bodily injury will result in the flesh-and-blood world. Because we rely so heavily on computer systems to provide basic services such as electric power, telecommunications, and medical care, disruption of those systems can have a catastrophic effect. Current federal law does not adequately punish those who damage computers resulting in death or serious bodily injury. Although statutes severely punish foreign terrorists who commit such acts, there is no parallel provision for domestic actors. Section 106 would close that loophole.

To protect Americans against the risk that damage to a critical computer system might threaten their health or safety, however, the Committee may want to consider broadening slightly the scope of Section 106 so that it covers not only hackers who damage a computer system *knowing* that death or serious injury will result, but also hackers who damage a computer system *with reckless disregard* for whether death or serious injury will result.

In an era in which computer systems play an integral role in our critical infrastructures, it is not difficult to imagine an assault on such a system that recklessly causes death or serious injury. Consider, for example, a hacker who infiltrates a hospital's medical database to erase records that reveal the diagnosis of his sexually transmitted disease. In the course of erasing his record, he also erases other patients' records, thereby preventing them from receiving vital medication or treatment. Although the hacker has not *intentionally* or *knowingly* harmed those other patients, his reckless conduct has clearly put them at risk of death or serious injury. If such reckless criminal conduct were to cause someone to die or to be permanently injured, the appropriate penalty might well exceed the ten-year maximum currently imposed by the statute.

Similarly, suppose a hacker shuts down a town's phone service. While phone technicians race to restore service, no emergency 9-1-1 calls can go through. It is easy to envision in such a situation that somebody might die or suffer serious injury as a result of this conduct. Although the hacker might not have known that his conduct would cause death or serious bodily injury, such reckless conduct would seem to merit punishment greater than the ten years permitted by the current statute.

The Internet is a powerful tool. But when the Internet is misused by criminals, it can turn into a harmful weapon. When criminals intentionally damage computer systems, recklessly causing severe harm or even death to others, they must be held fully responsible. Thus, the Department encourages the Subcommittee to expand the scope of Section 106 to encompass not only computer criminals who knowingly cause death or serious bodily injury, but also those who recklessly cause death or serious bodily injury.

II. SENTENCING GUIDELINES

Title I achieves another essential objective in the fight against computer crime by requiring the Sentencing Commission to re-examine the policy statements and guidelines that apply to computer crime. To guide the Commission in this endeavor, the Department recommends that Title I more clearly articulate its intent that the Commission enhance penalties to reflect the threat of computer crime. To that end, the Department outlines below three changes to Section 101 of the Bill.

First, Section 101 could better express the Bill's intent to raise penalties by directing the Commission to consider the fact that the USA PATRIOT Act increased the maximum penalties for many crimes involving unauthorized access to computers. For example, the USA PATRIOT Act doubled the maximum penalty for criminals and terrorists who cause damage to protected computers.

Second, the Bill's intent to enhance penalties would be emphasized if Section 101 required the Commission to examine the penalty structures that pertain to the disruption of computers that control our nation's critical infrastructures. Through the Internet, terrorists and criminals can attack the computer systems that control America's financial systems, power plants, health care providers, and transportation networks. Such attacks have the potential to cause grave economic disruption in addition to threatening American lives.

Third, we encourage the Subcommittee to impress upon the Commission the need for increased penalties by requiring it to consider harm to individuals. The Guidelines should take into account what this Bill already recognizes: where hackers cause death or bodily injury, they should face appropriately tough sentences.

In sum, Congress has already recognized the need to enhance penalties for cyber-crime; Section 101 should clearly express Congress' intent that the Sentencing Commission commensurately enhance such penalties.

III. EMERGING ISSUES

With the help of the Chairman and this Subcommittee, Congress has made great strides to modernize the laws that relate to the investigation and prosecution of cyber-crime. We look forward to continuing to work with the Subcommittee to address new issues as they arise in this evolving area of the law. With that in mind, I would like to share with the Committee a few issues forming on the horizon.

Concerns have been raised about the Department's ability under the current statutory scheme to assist other countries in foreign terrorism and criminal investigations when there is not an active corresponding investigation in the United States. Our continuing cooperation with foreign law enforcement agencies is essential, however, if we expect them to support our own requests for information and evidence found within their borders.

The Department has also been concerned for some time about the adequacy of the penalties imposed upon those who violate the privacy of others by intentionally intercepting their cellular phone calls. Today, such privacy invasions are treated as a minor infraction punished only by a fine. As cell phone use becomes more and more prevalent, however, it is increasingly important to protect the privacy of all wire and electronic communications without regard to the transmission technology used.

Finally, we are concerned about law enforcement's ability to respond to computer attacks in emergencies that involve a threat to a national security interest or an ongoing cyber-attack on a computer that controls a national critical infrastructure. Timely use of a pen register or trap and trace device may be the only way to identify the perpetrator of such an attack or to prevent the attack from causing further harm. Yet current law may not allow emergency use of such devices under these circumstances.

IV. CLOSING

Mr. Chairman, that concludes my prepared statement. I would like to thank you and the Subcommittee again for soliciting the Department's views on these important issues and for allowing me to express them through my testimony here today. I would be pleased to answer any questions that you may have on Title I of the Bill.

Mr. SMITH OF TEXAS. Ms. Koeppen.

STATEMENT OF SUSAN KELLEY KOEPPEN, CORPORATE ATTORNEY, MICROSOFT CORPORATION

Ms. KOEPPEN. I will strive to do the same, Mr. Chairman. Mr. Chairman and Members of the Subcommittee, it is my pleasure to testify this afternoon in support of H.R. 3482, and I would also like to commend you on your leadership for sponsoring this bill.

I am a corporate attorney at Microsoft focusing on legal issues surrounding security and cyber crime, but from 1994 to 1999, I was a Federal prosecutor at the Department of Justice Computer Crime and Intellectual Property Section. This afternoon, I would like to tell you why security has become Microsoft's top priority, why we feel cyber crime is such a serious problem, discuss sections 101 and 102 of the bill and offer an additional proposal regarding the forfeiture of personal computers used in cyber crime.

As an industry leader, Microsoft takes security very seriously. Every few years, Bill Gates sends an e-mail to the entire company that sets the course for all employees, and as you noted, Chairman Smith, in this year's e-mail, he places security as one of our top priorities as part of something we call trustworthy computing. Based on his direction when faced with a choice between new features or security, we will choose security in developing new products. We

see our role in creating more secure software as one element among many in this fight against cyber crime.

One of the reasons that we need H.R. 3482 is because in the online world, we don't treat cyber crime like real crime, and we don't treat cyber criminals like real criminals. No software, no operating system is immune from attack. The "I Love You," "Ramen," "Lion," "Code Red" and "Trinoo" attacks harmed different operating systems. They caused billions of dollars in losses and disruption to e-business and e-government.

Despite these costly and highly publicized online attacks, punishment has not always fit the crime. As a former Federal prosecutor, I speak from my own experience in saying that cyber criminals often don't get punished, because the applicable sentencing guidelines focus primarily on economic harm, which is often difficult to calculate and may not reflect the true harm caused.

Because these crimes do not merit stiff sentences, they may, in turn, not be investigated or prosecuted. Section 101 of the bill would change this by directing the Sentencing Commission to promulgate a guideline that enables judges to consider several additional factors so they have a better picture of the true harm caused by computer crime and a greater range of sentencing options. We strongly support section 101 and believe it will significantly help create a meaningful deterrent to cyber crime.

An important part of our trustworthy computing initiative is ensuring the privacy of our customer's information. Existing law provides that Internet service providers shall not divulge to anyone the contents of a communication held in electronic storage, but existing law creates an exception permitting disclosure in emergency situations. Our concern, however, is that ISPs may be constrained in making decisions in good faith to disclose information in an emergency situation. Section 102 makes several important improvements to existing law that will enable providers to make decisions promptly and without hesitation in emergency situations.

We are mindful that this is a sensitive area that needs to strike a delicate balance. We are eager to work with the Committee and other entities, such as the Center for Democracy and Technology, to find this balance.

One provision not in the current bill that we believe would help deter cyber crime is one which would permit criminal and civil forfeiture of personal equipment used to commit computer crime. We think forfeitures should apply to personal property that is used, or intended to be used, to commit a computer crime. The deterrent effect of expanded forfeiture for computer crime will be significant, particularly in cases of felons who attack cyber systems, not for personal gain, but merely for malicious effect.

In conclusion, we need H.R. 3482. Despite billions in cyber crime damage, many criminals remain at large. We worry that some may be the instruments of terrorist organizations or hostile nations. This is a risk we face, and we must take steps now to deter these actions.

Like traditional crime, cyber crime needs to be imposed with strict criminal laws, tough criminal penalties, strong enforcement capabilities and well equipped and highly trained law enforcers.

That is why we support H.R. 3482 and commend you, Mr. Chairman, for introducing this bill. Thank you.

Mr. SMITH OF TEXAS. Thank you, Ms. Koeppen.

[The prepared statement of Susan Kelley Koeppen follows:]

PREPARED STATEMENT OF SUSAN KELLEY KOEPPEN

INTRODUCTION AND SUMMARY

Mr. Chairman and Members of the Subcommittee, it is a pleasure to testify this afternoon in support of H.R. 3482, the "Cyber Security Enhancement Act of 2001."

My name is Susan Kelley Koeppen and I am a Corporate Attorney in the Microsoft Corporation's Product Development & Marketing E-Commerce Section. At Microsoft I focus on the legal issues surrounding electronic commerce, including security and cybercrime. From 1994–1999, I was a federal prosecutor at the U.S. Department of Justice in the Computer Crime and Intellectual Property Section. While at the Department, I investigated and prosecuted computer intrusions, economic espionage, and intellectual property crime, and helped develop government policy on critical infrastructure protection, cyber-terrorism, and encryption. I also served as an attorney advisor on intelligence policy.

This afternoon I would like to:

- emphasize that cyber crime is real and serious crime
- tell you why security has become Microsoft's top priority
- support Section 101 of the bill which gives judges greater direction in their punishment of cyber criminals by directing the U.S. Sentencing Commission to amend cyber crime sentencing guidelines
- support Section 102 of the bill which will enable Internet Service Providers acting in good faith to help the government in emergency situations involving danger of death or serious physical injury
- offer an additional proposal to strengthen the fight against cyber crime by permitting the criminal and civil forfeiture of computers and other equipment used to violate the Computer Fraud and Abuse Act.

CYBER CRIME IS REAL AND SERIOUS CRIME

In the online world, we often face a problem with criminal actions that are not treated as crimes, and with criminals who do not do time. While our society does not tolerate people breaking into brick-and-mortar homes and businesses, we inexplicably seem to have more tolerance for computer break-ins. Yet breaking into computers is just as much a crime as breaking into homes and businesses. Both break-ins harm innocent people and weaken American businesses, and computer attacks need to be treated as the truly criminal activities that they most assuredly are.

In the last few years, we have realized that the issues posed by criminal hackers are real, cross-platform, and costly. The "*ILOVEYOU*" virus of 2000 slowed down worldwide e-mail. The *Ramen* and *Lion* worms attacked Linux software to deface websites and extract sensitive information such as passwords. The *Code Red* worm exploited Windows server software to deface websites, infect servers, and attack other websites. The *Trinoo* attacks exploited vulnerabilities in the Solaris operating system to stage distributed denial of service attacks against several prominent websites. Estimated damage in these attacks runs into the billions of dollars.

As my former colleague Howard Schmidt likes to say, these attacks are genuine "weapons of mass disruption." Yet these attacks did not occur because the extremely innovative engineers creating the underlying codes disregarded security. They occurred because equally innovative criminal hackers worked day after day to find, create and exploit vulnerabilities in the software or in human nature that gave them new ways to trespass on your computers, steal your data and shut down your networks.

CYBER SECURITY HAS BECOME MICROSOFT'S TOP PRIORITY

As an industry leader, we have an important responsibility to lead on security issues. For many years, Microsoft has been in the forefront of industry efforts to increase the security of computer programs, products and networks; improve industry response to security breaches; enhance industry coordination with law enforcement; and better protect our critical information infrastructures.

Our senior executives are personally involved in this effort. Bill Gates, our Chairman and Chief Software Architect, is a presidentially-appointed member of the National Infrastructure Assurance Council (NIAC). The NIAC will advise the President and encourage cooperation between the public and private sectors to address physical threats and cyber threats to the Nation's critical infrastructure. Craig Mundie, Microsoft's Senior Vice President and Chief Technical Officer for Advanced Strategies and Policy, was appointed by the President to the National Security Telecommunications Advisory Council (NSTAC). The NSTAC advises the President on policy and technical issues associated with information infrastructure security. Steve Lipner, Microsoft's Lead Program Manager for Security, serves on the congressionally-mandated Computer Systems Security and Privacy Advisory Board. I am also pleased to be able to report that Scott Charney, former Chief of the Computer Crime and Intellectual Property Section at the Department of Justice when I served there, joins us on April 1st as our Chief Security Strategist, replacing Howard Schmidt, who has just joined the National Security Council staff under Richard Clarke, the President's cyber security advisor.

At their direction, we have taken many steps over several years to address security matters. This includes helping to found the IT-ISAC and the Partnership for Critical Infrastructure Security, and supporting White House Cyber Space Security Advisor Dick Clarke's new National Cyber Security Alliance which serves to educate home users on good security practices.

We also formed what we believe is the industry's best security response center, which investigates all reported vulnerabilities in our products, then builds and disseminates any needed security updates. In 2000, for instance, we received and investigated over 10,000 reports from outside sources. Where we found vulnerabilities—as we did in only 100 cases across all of our products and services—we delivered updated software through well publicized web sites and our free mailing list to 200,000 subscribers.

In another key security element, we announced at our second annual Trusted Computing conference a new partnership that will create best practices for handling product vulnerability information. We have agreed with several other companies, that the public release of vulnerabilities, also known as “exploit code,” before a patch is available is harmful to customers and inconsistent with professional responsibility if done while a vendor is creating the patch. Some firms or individuals release exploit code before there is a patch, and the end result is an increase in one's exposure to attack. [We believe that reaching a broad consensus for responsible reporting practices can improve both security awareness and lead to real security improvements.

Transcending all these past efforts was the recent decision to make “Trustworthy Computing” the company's highest priority. In a January e-mail, Bill Gates issued a call to action to all Microsoft employees—from developers, testers, customer support, to all executives—to make the hallmarks of a trustworthy computing experience our top priority—including security, availability and privacy in the way we design, test and support our products and services.

Operating system software is one of the most complex things humans have ever created, and there will never be software without vulnerabilities. While Bill's comments reflect many of the things we have already done to build more secure software, they also recognize what we have learned from the September's terrorist attacks as well as malicious and highly publicized computer viruses: We face great threats, and we have a role to play in ensuring the integrity and security of our critical infrastructures.

Part of this program includes a new customer service program called the Strategic Technology Protection Program (STPP). Through this initiative, we are helping our customers to “Get Secure” and “Stay Secure” so they have the most recent versions of patches and so they know how to manage their security needs going forward. This includes a toll free hotline that provides immediate assistance in dealing with viruses and more advanced development processes that will help reduce subtle flaws that can create vulnerabilities.

Another major element of our protection efforts focuses on incorporating new security features in our products. For example, we integrated previous stand-alone patches in products like Outlook 2001, installed a personal firewall in Windows XP, enabled users to have security patches downloaded automatically through the Windows Update tool, and added software restriction policies to Windows XP to allow administrators to limit what software can run on the system.

In the past, Microsoft has made software and services more compelling for users by adding new features and functionality, and by making our platform richly extensible. We've done a terrific job at that, but as Bill Gates noted, all those great features won't matter unless customers trust our software. So now, when we face a

choice between adding features and resolving security issues, we will choose security.

JUDGES NEED TO RECOGNIZE THE SERIOUSNESS OF COMPUTER CRIME

As a technology company, we, like many of our competitors, are doing all that we can to fight criminal hackers through superior technology and the initiatives mentioned above. Yet as a former federal prosecutor, I can tell you that nothing puts a chill on aggressive enforcement of a law than obtaining a conviction which then goes unpunished or under-punished. Unfortunately, that is the case today with respect to many computer crimes. Currently, sentences for violations of the Computer Fraud and Abuse Act (18 U.S.C. 1030) are determined primarily by calculating actual economic loss, which is often difficult to determine in the computer crime context. As a result, defendants convicted of computer crimes often serve little or no term of imprisonment. Not only is there no justice, but the deterrent effect from bringing the case evaporates and it makes computer crimes less likely to be prosecuted in the future.

Section 101 of the bill directs the Sentencing Commission to promulgate a guideline specifically addressing computer fraud and abuse. The Sentencing Commission, in determining the appropriate sentence for computer crime, is to consider a number of factors in order to create an effective deterrent to computer crime, including:

- the level of sophistication and planning involved in such an offense;
- whether or not such an offense was committed for purposes of commercial advantage or private financial benefit;
- whether or not the defendant acted with malicious intent to cause harm in committing such an offense;
- the extent to which such an offense violated the privacy rights of individuals harmed by the offense;
- whether the offense involved a computer used by the Government in furtherance of national defense, national security, or the administration of justice.

We believe individual cyber crimes need to be viewed in the context of the overall incidence of such offenses and the extent to which they constitute a threat to civil peace and economic prosperity. Cyber crime will never be effectively curbed if society continues to treat it merely as pranksterism.

We want sentences to take into account the persistence and skill applied by felons in the destruction, disruption or theft of information systems. We think it important that the invidious or destructive motives such violators pursue also be taken into account. It also is important that judges look not just at the monetary damage a violation may cause, but at the important intangible loss of personal privacy that often results from cyber crime. Finally, it is imperative that sentences reflect that any damage, tangible or intangible, to national security concerns or the delivery of needed government services is a loss to all society and must be punished.

By taking into account these additional factors, courts will have a better picture of the true harm caused by computer crime, and will have a greater range of sentencing options as a result. We strongly support Section 101 and believe that such sentencing guidelines will significantly help create a meaningful deterrent to cyber crime.

ISP'S MUST BE ALLOWED TO HELP IN EMERGENCIES

An important part of Trustworthy Computing is ensuring the privacy of users' information. We take this task very seriously, and we recognize that failures to provide privacy will undermine every attempt we make to build our consumer base for all products and services. We also work closely with entities such as the Center for Democracy and Technology to develop privacy enhancing tools and practices.

We believe existing law (the Electronic Communications and Privacy Act of 1986, 18 U.S.C. 2701 et. seq.) as recently amended by the PATRIOT Act (P.L. 107-56) correctly provides that those who offer electronic communication services to the public shall not knowingly divulge to anyone the contents of a communication held in electronic storage by that provider. The same prohibition on disclosure applies to those who provide remote computing services, if the provider is simply transmitting the information and has it for the purpose of providing storage or computer processing services to the user.

Exceptions include those situations where consent has been granted. Importantly, there is also an exception for disclosure to law enforcement agencies if the contents were inadvertently obtained and appear to pertain to the commission of a crime. Further, Congress has also added a provision that allows disclosure to law enforce-

ment where immediate danger of death or serious bodily harm requires disclosure without delay.

We support that provision added in the PATRIOT Act. Our concern, however, is that even under that provision (18 U.S.C. 2702(b)(6)(C)) communications providers or Internet Service Providers may be unnecessarily constrained in making decisions in good faith to disclose information in an emergency situation involving the danger of death or serious physical injury which requires immediate disclosure of that information. Section 102 makes several improvements to existing law that will enable such providers to make decisions promptly and without hesitation in emergency situations.

First, Section 102 permits disclosure of the contents of a private electronic communication when a good faith judgment has been made that there is an emergency involving a threat to life or serious bodily injury. We believe this is an appropriate adjustment in legal standards because there is a strong public interest in prompt decision making in such cases. Providers must feel free to use their best judgment without fear that their decision inevitably will be litigated afterwards.

Second, we believe that it is appropriate that the emergency disclosures contemplated by Congress need not be limited solely to law enforcement personnel, and this is consistent with the provision in the ECPA regarding emergency disclosure of subscriber information and records. Section 102 permits any government entity to receive such emergency disclosures of the contents of communications, just as they can now receive emergency disclosures of subscriber information and records. We believe that such emergency situations will be rare, but that law enforcement personnel may not always be reachable or even the best prepared to take immediate action. We think it appropriate that any government entity in a position to act to deter the threat of serious harm or death ought to be notified. Thus fire fighters, emergency response personnel, even school principals may be appropriate recipients of mortal threat information.

We are mindful that this raises concerns among some, and we look forward to working with Congress and others to strike the delicate balance that is required.

STRENGTHEN THE BILL BY INCLUDING THE FORFEITURE OF ASSETS USED TO COMMIT CYBER CRIME

One provision not in the current bill, but which we believe would help deter cyber crime, is one which would permit criminal and civil forfeiture of personal equipment, including computers used or intended to be used to violate or facilitate the violation of the Computer Fraud and Abuse Act.

Today, only the proceeds of an actual computer crime can be forfeited to the government. The actual means to commit those crimes are not.

Under existing law, both real and personal property which is derived from proceeds traceable to a violation of section 18 U.S.C. 1030 is subject to both criminal and civil forfeiture. See 18 U.S.C. § 981(a)(1)(C) & 982(a)(2)(B). Criminal forfeiture additionally will reach the proceeds of conspiracy to commit computer crime, but not attempted violations, nor are the actual tools of crimes or attempted crimes subject to seizure. Microsoft strongly supports the seizure of the proceeds of computer crime, but we urge that forfeiture also apply to any personal property, such as computer equipment, used or intended to be used in the commission of such crimes.

We propose clarifying in section 1030 itself that forfeiture applies to personal property that is used or intended to be used to commit or to facilitate the commission of a computer crime. We believe the deterrent effect of expanded forfeiture for computer crime will be significant, particularly in the cases of felons who attack cyber systems for malicious effect, but not personal gain. If the government can take away the means of the commission of cyber crime, it can complement the threat of conviction and jail time to law breakers in cyber space. In some cases, loss of personal computer equipment may actually be a stronger deterrent.

OTHER GOVERNMENT ACTION CAN HELP TOO

In addition to passage of H.R. 3482, there are other things government can do to promote cyber security. Microsoft supports:

- increased funding for law enforcement personnel, training, and equipment to investigate and prosecute cyber-crimes. These hard working officials are often short-staffed and under-funded. Many also lack the state-of-the-art technology used by hackers, and increased funding is needed to modernize and place them on par with those they investigate. There is also a role for hiring experts in cyber security as well as funding state and local law enforcement efforts to deter, investigate and prosecute cyber-security offenses.

- greater international cooperation among law enforcers in these time-sensitive investigations. Cyber-criminals and cyber-terrorists operate across international borders, as in the “ILOVEYOU” virus, the “Solar Sunrise” attack, and the “Anna Kournikova” virus. Enhanced international law enforcement cooperation is a vital tool our law enforcers need to fight and find the cyber criminals and cyber-terrorists. We also see the clear need for an international law enforcement framework that establishes minimum liability and penalty rules for cyber-crime. Without this, all the computer crime laws on the books are useless when cyber-criminals cross international borders.
- legislation to facilitate cyber security information sharing by: granting an exemption from the Freedom of Information Act (FOIA) for such information voluntarily shared with the federal government. This legislation will lead many companies to answer the government’s urging that they provide much more computer security data to the government. When that happens, the government network administrators will learn much more about network vulnerabilities from the private sector and be in a far better position to secure their own networks. They will also be able to model future attacks and position themselves to anticipate them in advance, whereas today most analysis occurs after the attack.

WE NEED H.R. 3482

Despite billions in cyber crime damage and significant network disruption, many criminal code writers remain at large. In this troubled time, we also can expect that some may fall under the control of terrorist organizations and hostile nations. Although the recent horrific terrorist attacks in New York and Washington were physical in nature, Congress quite rightly must look beyond the current tragedy and loss of those catastrophic attacks. We were fortunate that the terrorists or a random hacker did not unleash a corresponding cyber attack. Yet that is a risk we face, and we must take steps now to deter these actions.

Like traditional crime, cyber-crime needs to be opposed with strict criminal laws, tough criminal penalties, strong enforcement capabilities, and well-equipped and highly trained law enforcers.

That’s why we seek clear guidance from the Sentencing Commission on how courts should punish these convicted felons. That’s why we want ISPs to have the authority to share information voluntarily with the entire government once they see that life or limb are endangered. That’s also why we support tougher forfeiture provisions for criminal hackers. That’s why we support H.R.3482 and commend you, Mr. Chairman, for introducing this bill. This bill reflects a strong affirmation that cyber crime is just as dangerous to society as physical destruction through terrorism, arson or vandalism. It needs to be punished more severely, and Title I takes us in the right direction.

Thank you.

Mr. SMITH OF TEXAS. Mr. Smith.

**STATEMENT OF CLINT SMITH, VICE PRESIDENT AND CHIEF
NETWORK COUNSEL, WORLDCom**

Mr. SMITH. Mr. Chairman, Mr. Ranking Member, Members of the Subcommittee, my name is Clint Smith. I am the current President of the U.S. Internet Service Providers Association. USISPA member companies include America Online, Cable & Wireless, EarthLink, eBay, BCE Teleglobe, Verizon Online and WorldCom, where I work. Our association provides a forum for the ISP community to develop solutions to the critical issues that affect our industry. Cyber security is one such issue, and we are grateful for this opportunity to testify on H.R. 3482.

USISPA strongly supports 3482, and for the reasons set out in my testimony, we believe its enactment would increase Internet security and help deter cyber attacks.

We support H.R. 3482 for three reasons: It increases funding for law enforcement; it strengthens penalties for cyber crime; and it reduces potential impediments to ISP corporation with law enforce-

ment. I will discuss each of these three items in turn and then discuss one provision in the bill that USISPA would like clarified.

First, we endorse the increased funding for the fight against cyber crime. We work with law enforcement agents every day on cyber crime investigations, and they need more resources. We commend section 104 for authorizing the National Infrastructure Protection Center and appointing NIPC as a focal point for security threat assessments and education.

NIPC has some of the world's best security experts, and it is uniquely positioned to serve as a national focal point for this work.

With respect to penalties for cyber crime, we support section 101 and the amendment to the sentencing guidelines. We also are strong supporters of section 106. Mr. Chairman, as you mentioned in your opening statement, online crime can result in physical injury or death in the offline world. Hospitals, airlines, railroads, energy companies all rely on computer networks, and a disruption in their networks will disrupt their organizations and could result in physical injury or death. Section 106 is good policy.

Let me turn to cooperation between ISPs and law enforcement. H.R. 3482 contains important provisions that if enacted, will reduce existing impediments to ISP cooperation with law enforcement. Cyber security cannot exist without cooperation between service providers and law enforcement.

Let me touch on two points of the bill that we think are very important. Existing law, as Ms. Koeppen mentioned, authorizes an ISP to disclose customer records or communications if the ISP reasonably believes that there is an immediate risk of death or personal injury, such as with an e-mail bomb threat. This was a positive change in the law, but it put ISPs in an odd position. We have to determine when a threat is immediate, and we have to establish that we have a reasonable belief in the credibility of that threat.

Let me pose a hypothetical. Tonight an ISP is notified that someone in one of their chat rooms claiming to be a fourth grader intends to blow up his school with a bomb on March 15. The ISP has to decide March 15; that is more than a month away. Is that an immediate harm that I am authorized to report under this section? The ISP has to think a fourth grader gaining access to a bomb. Is that a reasonable belief that I have about this threat? And our point here is that the ISPs are being put in the position to make a judgment about the timing and the credibility of a threat that ought to be made by law enforcement. And so we support your bill that changes the standard to a good-faith standard and removes the immediacy requirement, because it is good policy for ISPs to report this type of threat to law enforcement rather than make a judgment as to whether it should be reported.

The second point relating to cooperation between ISPs and law enforcement relates to the immunity that is provided to service providers when cooperating with law enforcement. H.R. 3482 clarifies that ISPs are immune from liability for acting in good faith, one, when they turn over information to law enforcement in an emergency situation such as the chat room bomb threat I just mentioned, and second, when they invite law enforcement to monitor communications of a computer trespasser.

Let me offer a second hypothetical. If tonight an ISP identifies a trespasser on their systems and they invite Government experts in to help them conduct surveillance to catch that trespasser, that trespasser could sue the ISP under various legal theories under contract law, under a violation of the ISP's privacy policy, under a theory of trade secret theft. The trespasser could bring causes of action against the ISP relating to the very activity that the USA Patriot Act was trying to encourage. Your bill, H.R. 3482, in creating immunity for ISPs when cooperating and tracking a computer trespasser with law enforcement, is consistent with equivalent statutory immunities applying to electronic surveillance conducted under other statutory authorization, and it is good public policy. Making this immunity explicit will remove an ambiguity in the current law that might otherwise reduce cooperation between ISPs and law enforcement.

My last point is a part of the bill that we think requires some clarification, and that is section 105, relating to Internet advertising of illegal devices. In our view, this section of the bill leaves it unclear whether an ISP, a portal like a Yahoo, a third-party transaction site like an eBay or an online directory company like a yellow pages would have some criminal liability or an obligation to take down content that advertise such a device. We ask this Committee to clarify that section 105 neither requires our members in any way to monitor traffic or to screen or filter content nor restricts our members from doing so when that is appropriate.

In conclusion, I believe the successful investigation and prosecution of crime on the Internet requires a legal framework that balances the powers of law enforcement, the privacy rights of individuals and the responsibilities and liabilities of service providers. The members of the USISPA commend the authors of H.R. 3482 for finding an appropriate balance of these interests in their legislation. We urge the prompt consideration and passage of this bill.

Mr. SMITH OF TEXAS. Thank you, Mr. Smith.

[The prepared statement of Mr. Smith follows:]

PREPARED STATEMENT OF CLINT N. SMITH

INTRODUCTION

Mr. Chairman, Mr. Ranking Member, members of the Subcommittee, my name is Clint Smith. I am the current President of the U.S. Internet Service Providers Association ("USISPA").

USISPA, based in Washington D.C., is a 501(c)(6) trade association for Internet service providers. Member companies include America Online, Cable & Wireless, EarthLink, eBay, BCE Teleglobe, Verizon Online, and WorldCom, where I work as the Vice President and Chief Network Counsel. Our association provides a forum for the ISP community to develop solutions to the critical issues that affect our industry. Cyber security is one such issue, and we are grateful for this opportunity to testify on HR 3482, "The Cyber Security and Enhancement Act of 2001."

USISPA strongly supports HR 3482 and, for the reasons set out in this testimony, believes its enactment would increase Internet security and help deter cyber-attacks.

BACKGROUND: THE USA PATRIOT ACT

HR 3482 builds upon the legal foundation set out in the USA Patriot Act, Public Law 107-56. The ISP community generally supported the USA PATRIOT Act. We greatly appreciated the efforts made by the legislation's authors in Congress and all interested parties to draft that law under tight deadlines and extraordinary circumstances.

As would be expected from such an accelerated process, the USA PATRIOT Act contained some ambiguities and generated questions for ISPs. In our view HR 3482 clarifies these points and, in doing so, will further the objectives of the USA PATRIOT Act.

USISPA collectively supports HR 3482 for three reasons:

- It increases funding for law enforcement,
- It strengthens penalties for cybercrime, and
- It reduces potential impediments to ISP cooperation with law enforcement.

In my allotted time, I will discuss each of these three items in turn and then discuss one provision in the bill that USISPA would like clarified.

NATIONAL INFRASTRUCTURE PROTECTION CENTER

First, USISPA endorses the increased funding for the fight against cybercrime provided by HR 3482.

- Section 104 of the bill provides for the authorization of \$57.5 million for fiscal year 2003, to be appropriated to the National Infrastructure Protection Center (“NIPC”). This funding would assist NIPC to serve as a national focal point for security threat assessments and warnings, and to coordinate responses to attacks on the country’s critical infrastructure.

PENALTIES FOR CYBERCRIME

USISPA also endorses the bill’s strengthened penalties for cybercrime.

- Sec. 101 would authorize the amendment of the federal sentencing guidelines to encompass a wider range of criteria when sentencing cybercriminals. We commend the bill’s authors for expressly identifying for harsher punishment (1) acts done with malicious intent to cause harm and (2) offenses that violate the privacy rights of individuals.
- Section 106 amends title 18 U.S.C. §1030(c) to allow for criminal penalties to be increased if the offender knowingly causes or attempts to cause death or serious bodily injury through a cyber attack.

Increased penalties provided for in HR 3482 could deter would-be hackers, benefiting law enforcement, the public, and the ISP industry.

ISP COOPERATION WITH LAW ENFORCEMENT

HR 3482 contains important provisions that, if enacted, will reduce impediments to ISP cooperation with law enforcement.

Service providers and law enforcement agencies form an essential partnership in fighting cybercrime. Cyber security cannot exist without that cooperation. It is important that the legal framework for ISP interaction with law enforcement is clear because ambiguities will create impediments to cooperation on an important investigation. HR 3482 would clarify ambiguities in the existing legal framework by making the following amendments to current law:

- First, the USA PATRIOT Act authorized an ISP to disclose customer records or communications if the ISP *reasonably* believes there is an *immediate* risk of death or personal injury, such as with an email bomb threat. This was a positive change for both law enforcement and ISPs. But it put ISPs in the odd position of having to determine whether the danger was “immediate,” and the “reasonable” belief standard may require an ISP to research whether an emergency situation is a bona fide emergency prior to alerting law enforcement. HR 3482 removes the requirement that the danger be “immediate” and allows ISPs to act on a “good faith” belief rather than the higher standard of a “reasonable” belief. These changes will encourage ISPs to promptly report threats of death or personal injury to law enforcement.
- The USA PATRIOT Act expanded law enforcement investigative powers to fight terrorism but did not explicitly grant ISPs immunity from liability in all cases for their role in this fight. HR 3482 clarifies that ISPs are immune from liability for acting in good faith (1) when they turn over information to law enforcement in emergency situations and (2) when they invite law enforcement to monitor the communications of a computer trespasser. Equivalent statutory immunity applies in other contexts involving ISP involvement in electronic surveillance conducted under statutory authorization. Making such immunity explicit will remove an ambiguity that might otherwise reduce cooperation between ISPs and law enforcement.

INTERNET ADVERTISING OF ILLEGAL DEVICES

While USISPA endorses HR 3482 generally, and specifically supports the preceding sections of Title I relating to cybercrime, one provision deserves fine-tuning to avoid ambiguity and ensure that those who merely act as conduits for information—such as ISPs, portals, third-party transactions sites, and online directory companies—are not inadvertently exposed to liability.

Specifically, Section 105 (“Internet Advertising of Illegal Devices”) of HR 3482, in our view, leaves it unclear whether the modifications to 18 USC §2512(c) would make ISPs, portals, third-party transactions sites, online directory companies or other Internet advertisers liable when illegal monitoring and wiretapping devices are advertised on their networks or through their services. While we recognize that this may not be the intent of the legislation, USISPA urges this committee to clarify that Section 105 neither requires our members, in any way, to monitor traffic or to screen or filter content nor restricts our members from doing so.

CONCLUSION

The successful investigation and prosecution of crime on the Internet requires a legal framework that balances the powers of law enforcement, the privacy rights of individuals, and the responsibilities and liabilities of service providers. The members of USISPA commend the authors of HR 3482 for finding an appropriate balance of these interests in their legislation.

We urge prompt consideration and passage of HR 3482.

Mr. SMITH OF TEXAS. Mr. Davidson.

**STATEMENT OF ALAN DAVIDSON, STAFF COUNSEL, CENTER
FOR DEMOCRACY AND TECHNOLOGY**

Mr. DAVIDSON. Mr. Chairman and Members of the Subcommittee, thank you very much for calling this hearing. We very much appreciate the opportunity to testify on H.R. 3482.

I am Alan Davidson, Associate Director of the Center for Democracy and Technology, a public interest nonprofit group based here in Washington that focuses on promoting civil liberties and human rights on the Internet.

In the aftermath of September 11th, it is more clear than ever that cyber security is a serious problem that demands a real response from Government. At the same time, such responses must be respectful of the protections for personal privacy enshrined in our Constitution and in our electronic surveillance laws. If we are forced to give up these essential liberties fundamental to our American way of life, then our country will truly have lost something important. It is in this context and with this in mind, this need to protect both security and privacy, that we offer the following three comments on the bill.

First, Mr. Chairman, my organization has never been shy about pointing out bills that raise serious privacy concerns. This is not one of those bills, with one exception, which I will speak about, section 102, the emergency disclosure provision, and we appreciate the chance of this hearing and also your measured response in terms of dealing with this serious issue.

I will focus my remarks then, on section 102 and on the—some of the things that we believe the Committee could do otherwise. The emergency disclosure provision of section 102 as drafted currently is overly broad, and we fear would eviscerate some important privacy protections that exist in the law right now.

Right now emergency disclosure provisions exist based on this idea, that ISPs who encounter material that—where they believe there is an imminent danger of threat—or threat of serious injury

or death, can contact and reveal those communications to law enforcement agencies. In practice, what we are hearing in the field is that that is not exactly the way it works. More and more what we have heard from ISPs, from other providers like libraries, universities, the way this interaction happens is that a law enforcement official will come to the provider and say, we have reason to believe that there is something—that there are communications that we need access to that will reveal information about an imminent threat of death or serious injury and will you give us this information. And the providers are left with this Hobbesian choice, either protect the privacy of their subscribers or say no—I'm sorry, reveal these sensitive communications to law enforcement or have to say no to law enforcement, and nobody wants to say no to law enforcement, certainly not in this environment.

And our fear is that these voluntary disclosures are turning into a major loophole in current law, because small providers are not in a position to evaluate these requests when they come, and of course, just turn around and provide this information.

There are some major differences in the provision in section 102 versus the provision that was passed just 4 months ago in the USA Patriot Act. The biggest one, I think the most important one, is the breadth of the entities to which this information can be revealed. Any governmental entities, not just law enforcement agencies. That is, literally thousands of Federal employees, State and local government employees, potentially even foreign government entities who could have access to this information or this information could be revealed legally.

The issue with imminent danger I think is an extremely important provision that has been dealt with in a lot of the emergency disclosure rules that exist, and it is an important protection in terms of making sure that this is not just about a hypothetical danger, but a reasonable imminent danger that needs to be dealt with.

So we urge the Committee to rethink this expansion. It is our belief that, in fact, there are ways to craft this carefully, and we look forward to working with the Committee and members of industry to find ways to meet these needs.

The third point we wanted to make is that we urge the Committee to continue its work to balance powerful surveillance authorities with appropriate privacy protections. The USA Patriot Act, which was passed this fall, provides substantial new Government capabilities to conduct surveillance on Americans. H.R. 3482 also provides additional and powerful new resources and tools, but in both cases there are virtually no new measures for accountability and oversight or any protections for the sensitive personal information that is increasingly available in the information age.

We urge the Committee to adopt a more comprehensive approach to cyber security that recognizes the additional need to provide privacy protections as we provide new law enforcement capabilities, and I have detailed, in my testimony, some of the very excellent provisions that this Committee itself adopted in the last Congress in H.R. 5018, and I think would go a long way toward providing that balance, including providing standards for access to the sensitive GO location information from cell phones, dealing with some

of the issues raised by pen/trap standards. There are others that I have listed in my testimony.

In conclusion, I would just say again, to recap that we urge the Committee to narrow the new emergency disclosure provision of section 102, to look back at H.R. 5018 and find ways to add some balance into these new authorities and capabilities that are being given to law enforcement. Powerful new Government surveillance and law enforcement capabilities demand powerful oversight and accountability and privacy protection mechanisms. We look forward to working with you and other Members to deal with that.

Mr. SMITH OF TEXAS. Thank you, Mr. Davidson.

[The prepared statement of Mr. Davidson follows:]

PREPARED STATEMENT OF ALAN DAVIDSON

Mr. Chairman and Subcommittee Members, thank you for calling this hearing and giving CDT the opportunity to testify on H.R. 3482, the "Cyber Security Enhancement Act of 2001."

I am Alan Davidson, Associate Director of the Center for Democracy and Technology, a public interest non-profit group based here in Washington. CDT works to promote civil liberties and human rights on the Internet. Since its creation in 1994, CDT has been heavily involved in the policy debates concerning privacy, computer security, and government surveillance online. As Staff Counsel I have led CDT's project on encryption policy and done substantial research on computer security and privacy based on my own training as a computer scientist. CDT also coordinates the Digital Privacy and Security Working Group, a collaboration of over 40 leading Internet companies and public interest organizations pursuing issues of privacy and security online.

Our nation is at a point where revolutionary changes in communications and computer technology have created new concerns about public safety, security, and privacy online. In the aftermath of September 11, cybersecurity is a serious problem that demands a real response from government. At the same time, such responses must be respectful of the protections for personal privacy and from overly broad governmental authority, enshrined in our Constitution and electronic surveillance laws.

If we are forced to give up essential liberties fundamental to our American way of life than our country will truly have lost something important.

With this need to protect both security and Constitutional privacy principles, CDT offers the following comments on H.R. 4382:

First, CDT commends this committee for holding this hearing, and for the relatively measured approach taken in HR 3482. We agree that computer crime and security is a serious problem that requires serious government response. In the USA PATRIOT Act, passed this fall, substantial changes were made to the computer crime and government surveillance statutes that raised serious privacy concerns and are to this date still not fully understood. In contrast and with one notable exception—the emergency disclosures provision of Section 102—H.R. 4382 takes a more modest approach to these laws that does not raise the same types of privacy concerns.

Second, the emergency disclosure provision of Section 102, as drafted, is overly broad and would eviscerate important privacy protections in current law.

Current law protects the privacy of electronic communications by prohibiting service providers from revealing those communications to anyone without proper lawful orders. Emergency disclosure provisions exist in the current law based on a reasonable idea—ISPs who reasonably believe there is an imminent threat of death or serious injury should be able to reveal communications to law enforcement agencies on an emergency basis even without judicial oversight.

Sec. 102 would substantially expand this ability to reveal private communications without any judicial authority or oversight.

In practice, however, we have heard reports from large and small providers, universities, and libraries, that the emergency disclosure is being used in a different way. Providers are often approached by government agents and asked to voluntarily disclose communications or other subscriber information for investigations that the government claims involve a danger to life and limb. Providers are then faced with a Hobbesian choice—either turn over sensitive private communications of subscribers without any court order, or say no to a government request. Of course many comply with the requests. Small providers have few legal resources to evaluate such

requests. Others receive requests from the same agents they may seek help from the next day regarding hacking attacks or other problems. Without proper restrictions, such “voluntary disclosure” provisions risk becoming a major loophole.

Current law, passed just four months ago, confines these extraordinary disclosures to law enforcement agents in limited circumstances. As drafted, Sec. 102 would threaten the privacy of communication by substantially broadening these disclosures:

- It allows these disclosures to *any* governmental entity, not just law enforcement agents. That could include literally thousands of federal, state, and local employees—perhaps even foreign government officials.
- It no longer requires *imminent* danger for disclosure. It would allow these extraordinary disclosures when there is some danger, which might be far in the future and far more hypothetical.
- It no longer requires a *reasonable belief* that there is a danger on the part of the ISP. Section 102 would allow these sensitive disclosures if there is any good faith belief—even if unreasonable—of danger.

Thus as drafted, Sec. 102 would allow many more disclosures of sensitive communications without any court oversight or notice to subscribers. It would allow these disclosures to (and based on requests from) potentially hundreds of thousands of government employees, ranging from local canine control officials to schoolteachers to Agriculture Department cotton inspectors to foreign government officials.

We urge the committee to carefully rethink this expansion. We understand the argument that in some *narrow* circumstances disclosures to some entities—such as the Center for Disease Control—might be warranted. As supported in current law, in cases of imminent threats of death or serious injury, law enforcement agencies—trained to deal with such situations and cognizant of legal strictures—should be the first contact point for concerned citizens. We also urge the committee to maintain the requirements of a reasonable belief in *imminent* danger.

We are confident that if other disclosures are needed they can be carefully crafted, and we look forward to working with the Committee as well as experts in industry and other interested parties to find a more balanced approach.

In addition, we strongly encourage this Committee to add accountability mechanisms for this extraordinary power. Congress should consider requiring notice to the subscriber, after the fact (and deferrable based on a judicial order), as a means of providing subscribers with some way of knowing that their communications have been disclosed. And at a bare minimum Congress should mandate a reporting requirement for these emergency disclosures to federal law enforcement, to give Congress some method of evaluating their use.

Third, we urge the Committee to continue its work to balance powerful surveillance authorities with appropriate privacy protections.

An essential element of security in cyberspace is trust. If Internet users cannot trust that their most sensitive personal and business communications will be private, then we cannot realize the promise of the Internet as a communications medium.

Powerful new surveillance authorities require powerful oversight and accountability. In addition, the digital age is making more personal information available than ever before, also increasing the need for a legislative framework that protects personal information from inappropriate surveillance.

The USA Patriot Act passed this fall provides substantial new government capabilities to conduct surveillance on Americans and to combat terrorism and cyber crime. H.R. 4382 also provides additional and powerful new resources and tools. But in both cases there are virtually no new measures for oversight and accountability, or any protections for all the sensitive personal information increasingly available in the digital and wireless age. (We note that this committee’s own admirable efforts to strike a greater balance in the PATRIOT Act were largely ignored.)

We urge this committee to adopt a more comprehensive approach to cybersecurity that recognizes the urgent need for additional privacy protections. The Congress could start by taking up the helpful changes to surveillance law developed and passed by the House Judiciary Committee in the last Congress, under H.R. 5018, including:

- Heightened protections for access to wireless location information, requiring a judge to find probable cause to believe that a crime has been or is being committed. Today tens of millions of Americans are carrying (or driving) mobile devices that could be used to create a detailed dossier of their movements over time—with little clarity over how that information could be accessed and without an appropriate legal standard for doing so.

- An increased standard for use of expanded pen registers and trap and trace capabilities, requiring a judge to at least find that specific and particularly facts reasonably indicate criminal activity and that the information to be collected is relevant to the investigation of such conduct.
- Addition of electronic communications to the Title III exclusionary rule in 18 USC §2515 and add a similar rule to the section 2703 authority. This would prohibit the use in any court or administrative proceeding of email or other Internet communications intercepted or seized in violation of the privacy standards in the law.
- Require statistical reports for §2703 disclosures, similar to those required by Title III.
- Require high-level Justice Department approval for applications to intercept electronic communications, as is currently required for interceptions of wire and oral communications.

In addition, other issues—some of broader scope—need to be addressed:

- Improve the notice requirement under ECPA to ensure that consumers receive notice whenever the government obtains information about their Internet transactions.
- Provide enhanced protection for personal information on networks: probable cause for seizure without prior notice, and a meaningful opportunity to object for subpoena access.
- Require notice and an opportunity to object when civil subpoenas seek personal information about Internet usage.

The bills put before this Committee last Congress were efforts towards a modest improvement in privacy protections without in any way denying the government any investigative tools. They should serve as a starting point, and we hope that you will consider including them to address the privacy concerns of many Americans and the imbalance that exists in today's electronic surveillance laws.

In conclusion, we urge to Subcommittee to

- Substantially narrow the new emergency disclosure provisions of Section 102. If retained, they should greatly limit the scope of governmental entities that can receive such disclosure, could provide deferred notice to the subscribers whose communications were revealed, and should absolutely require reporting to Congress on their use.
- Take a more balanced approach by including some of the privacy protections passed by this committee last Congress. Among the most urgent of these: a need for clearer protection of wireless location information, clearer definitions of what constitutes content for pen/trap orders online, and additional statistical reporting requirements.

Protecting national security and public safety in this digital age is a major challenge and priority for our country. On balance, however, we believe that new sources of data and new tools available will prove to be of great benefit to government surveillance and law enforcement. It is essential that we offer a measured response to these concerns, and urgently take up the need for additional privacy protections in the electronic surveillance laws.

Powerful new government surveillance and law enforcement capabilities demand powerful oversight, accountability, and privacy protection mechanisms. We look forward to working with the Subcommittee and other interested parties to craft an approach that protects both security and privacy online.

Mr. SMITH OF TEXAS. I am going to yield my initial time to the gentleman from North Carolina, the Chairman of the Intellectual Property and Internet Subcommittee, because I know he has another engagement he has to attend. So Mr. Coble you are recognized for your questions.

Mr. COBLE. Thank you for that courtesy, Mr. Chairman. I do have another meeting that starts in about 5 or 10 minutes. Good to have you all with us, by the way.

Mr. Davidson, in your testimony, you indicate that you have special concerns about section 102 and that the rest of the bill does not raise the same types of privacy concerns. Now, do I correctly

or accurately conclude that you have no problem with the rest of the bill?

Mr. DAVIDSON. Well, let me say that I think—first of all, as far as title II goes, I think our organization doesn't really have—has not worked in that area, doesn't really have a strong opinion about that issue in terms of the creation of these new centers within the Justice Department.

Mr. SMITH OF TEXAS. Mr. Coble, if he doesn't have a strong opinion, I take that as an endorsement.

Mr. COBLE. I was trying to lead him in that direction, but he—

Mr. DAVIDSON. Well, let me just say that I think we hope that there will be balance. These are certainly not the same level—honestly, I want to say that these are not the same level of concerns that were raised, for example, by the USA Patriot Act, and I hope that the Committee appreciates our candor in saying that even though there may be minor issues here, and I think that more probably are some and I hope that we will continue to provide more accountability mechanisms for law enforcement in exercising these authorities, but these are not the same things as the USA Patriot Act. I think it is important for Congress to know that.

Mr. COBLE. That is not an unreasonable response, Mr. Chairman. Mr. Scott, don't you agree?

Thank you, sir. The bill includes important provisions for combatting cyber crime and improving cyber security, it seems to me. And some of you have touched on this, but I want to give you another shot on it, starting, Mr. Malcolm, with you. What other steps, if any, do you think Congress should take in this area?

Mr. MALCOLM. Well, Congressman Coble, I believe that I mentioned several of them. However, there are a few that I would like to talk about. One of them deals with illegal wiretaps. Congress has gone a long way toward protecting the public against illegal wiretaps and unlawful access to stored communications. However, I do believe that two changes are appropriate for this Committee to consider. Under current law, Congressman, illegal interceptions of cellular telephone conversations are treated as mere infractions, subject only to a fine. Now, this might have been appropriate back in 1986 when the law was enacted and cell telephones were seldom used. However, that is no longer the case, and the Department believes that it no longer makes sense to treat the interceptions—illegal interceptions of cell telephone conversations any differently than illegal interceptions of any other electronic or wire communication.

As well, Congressman, another change is that with respect to invasions of privacy through hackers or system administrators working on an inside, improperly accessing communications that are in electronic storage, at the moment such invasions, while intensely personal—I mean, somebody can access your e-mail and read your communications about your family, communications with your accountant, communications with the doctor, communications with a lawyer. At the moment a first offense is treated as a 6-month petty offense, and if somebody acts with a malicious intent, say, to—or an aggravated intent in order to gain financially or maliciously destroy property, it is still a misdemeanor, subject to a 1-year penalty.

The Department believes that this does not provide adequate protection to individuals and believes that it would be appropriate in today's world if somebody accesses e-mail or stored communication improperly, that a first offense should be treated as subject to a penalty of up to a year and that if somebody acts with an aggravated mental state seeking commercial or financial gain, seeking to maliciously destroy property, acting with a criminal or tortious—in furtherance of criminal and tortious conduct, that that person ought to be subject to a 5-year penalty.

Another provision, Congressman, deals with how juveniles are treated in the law. Under current law—well, I should say adults who have juvenile records—I am not proposing—the Department is not proposing that juveniles be treated any differently. Under current law, if a first offender is an adult offender, they get treated to a certain penalty. This bill recognizes that people who recidivate should be treated more seriously. However, under current law, Congressman, juvenile adjudications of delinquency for hacking are not treated, for purposes of sentencing guidelines in the statute, as a prior conviction.

Mr. COBLE. All right. Now, my 5 minutes are about up. Anybody else want to be heard? Thank you for that, Mr. Malcolm.

Mr. MALCOLM. Sure.

Mr. COBLE. Any other panelist? Thank you, Mr. Chairman. Thank you.

Mr. SMITH OF TEXAS. Thank you, Mr. Coble. The gentleman from Virginia, Mr. Scott, is recognized for his questions.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. Malcolm, did I understand you to say that the 5-year penalty, does that have any effect on the Department's enthusiasm about prosecution?

Mr. MALCOLM. I am sorry. Congressman—

Mr. SCOTT. The enthusiasm for prosecution, does the Department of Justice more likely to go after somebody if you can get 5 years rather than the maximum 6 months?

Mr. MALCOLM. Yes, Congressman.

Mr. SCOTT. Okay. Ms. Koeppen, and I guess anybody, have you reviewed section 101 with the various concerns that we had asked the Sentencing Commission to consider, and are there other considerations that might be appropriate? And if you are not prepared to answer that now, if you could either later in the hearing or soon, I would like to hear—

Mr. DAVIDSON. I would be happy to provide some additional comments on this. We have provided some comments I think informally to staff, and there are other efforts underway, I believe, sentencing guidelines that need to be taken into account, and there are some issues that I think should be considered as well and we are happy to amend our testimony to add some of those comments.

Mr. SMITH. USISPA as well can submit some additional comments in writing. I would offer one right now, which would be the activity of sharing information with others who had the same malicious intent. We see quite a bit of activity in hacker discussion groups, in chat rooms, where an exploit in one person's hand is a nuisance. An exploit in 200 young hackers' hands is a catastrophe.

Mr. SCOTT. And I guess if you up load something or e-mail it to hundreds of people, it is worse than just one or two people looking at it?

Mr. SMITH. Yes, sir.

Ms. KOEPPEN. I will also submit personal comments.

Mr. SCOTT. Okay. Mr. Davidson, one of the things that you consider when you start looking in privacy is whether or not there was an expectation of privacy. Is there an expectation of privacy in a chat room?

Mr. DAVIDSON. I think that the answer was probably that it depends. But I think in a public chat room, it is a very different—it is a different expectation than——

Mr. SCOTT. So it is——

Mr. DAVIDSON. It is much more——

Mr. SCOTT. If you catch somebody in a public chat room, I mean, there is no expectation of privacy. You wouldn't have any—there wouldn't be any reason why you wouldn't share that information with law enforcement if you saw it.

Mr. DAVIDSON. Well, I think that ISPs are in a particular position under the law in terms of their—their special position with their customers in terms of collecting information. I am not exactly sure where you are going with this, but I guess the——

Mr. SCOTT. I guess some areas you get some information where there is an expectation of privacy and other areas there may not be. If there is no expectation of privacy, then, you know, we don't have a problem. If an e-mail—I would think there would be an expectation of privacy, and if the—so—somebody had gone into a little bit about—I think you had gone into information about how you get the information to begin with. There is a difference if the police come to you and say we are looking into activities of a certain person. Give us what you got is different than if you trip over some information yourself, for which particularly, there wasn't an expectation of privacy, there would be no problem in giving that information up. Your question would be when the police come and ask you for information which your customer might expect to be private.

Mr. DAVIDSON. Well, I think that there are going to be a lot of reasons that customers would expect their information to be private even in “chat rooms.” Recognize that some chat rooms might just be a couple of people, small private settings. Even chat rooms that might be open to lots of people, one might not expect their communications to be overheard. It is a very different situation than we have. I think the analogy in the real world is oh, gosh, you don't have any expectation of privacy, and your chat is on a street corner.

For example, that might be overheard by a passerby. At the same time, there is nobody on—who is sitting on every street corner monitoring every communication recording it like an ISP might be in a position to. So I think the analogies fail. I would have to think more carefully about whether or not there might be some situations where there is enough of a diminished expectation that we might not need these requirements that ISPs not provide the information without a lawful order, which I think may be what you are getting at.

Mr. SCOTT. Mr. Malcolm, how do the police determine when they ask for information and when they don't—I mean, do you wait for a little probable cause before you start asking for people's private information?

Mr. MALCOLM. I am a little bit unclear—

Mr. SCOTT. This bill would allow you presumably to start asking for people's private computer information, so long as the ISP can give it to you in good faith. That is not much of a standard.

Mr. MALCOLM. I fail to see that, Congressman, with all due respect, because there are still statutory standards that are set out before the ISP can provide the information, and if I could in that respect respond to Mr. Davidson, I don't believe that it is the situation that ISPs simply roll over whenever law enforcement contacts them. ISPs, when they are contacted by law enforcement, assuming that they have been contacted as opposed to coming forward with the information voluntarily, are supposed to act independently. They are supposed to act in good faith. There has to be a determination that an emergency exists. The determination about an emergency has to be that there is a threat—

Mr. SCOTT. Well, I think this bill recognizes the position that the ISP is in when a law enforcement officer says it is important I get the information. I mean—

Mr. DAVIDSON. That is enough. I mean, not to interrupt, Mr. Scott, but I think that that is exactly the situation that we are hearing about, especially with small ISPs and small providers who don't have legal counsel, who don't have the ability—and who want to do the right thing. I think people really want to do the right thing.

Mr. SCOTT. And so the screening ought to take place when law enforcement decides to ask.

Mr. MALCOLM. Well, Congressman Scott, first of all, I believe that it will be a rare circumstance if ever a circumstance would exist, when law enforcement would contact an ISP saying that we believe that there is an emergency situation going on, when, in fact, they have no such belief. Once law enforcement contacts the ISP, while the ISP may still want to do right, there is a statutory standard that is set in place.

The ISP is to make an independent judgment, and if they decide after making that independent judgment that they are not entitled in good faith to turn over that information, then law enforcement has no choice but to appropriate—

Mr. SCOTT. Well, if the ISP—if the law enforcement asks the ISP to give up the information, aren't they, per se, in good faith, by giving it up?

Mr. MALCOLM. Congressman, I believe—I am not meaning to get into a semantic distinction with you—law enforcement is not contacting an ISP saying I want information; give it up. They are contacting an ISP and saying, we believe, ISP, that an emergency situation exists. It is an emergency situation that involves a threat of death or serious bodily injury and that you must provide the information without delay or else grave consequences—

Mr. SCOTT. And the ISP would be in good faith just giving it up?

Mr. MALCOLM. No. The ISP, with all due respect, Congressman, is supposed to make an independent judgment as to whether those

circumstances exist, and if they, in good faith, believe that those circumstances exist, they provide the information.

Mr. DAVIDSON. This situation happens all the time, though and the only information that is available is the information that comes from law enforcement. I think the ISPs and the small providers—and again, we are talking potentially about libraries or State universities. And I have heard these stories where—sometimes foreign government entities will come and say we are investigating a case, a kidnapping, a serious thing, a potential terrorist act perhaps. But the cases that we have heard about are serious cases. They will say, we think we need information that you have, and the only thing that I think that—in the anecdotal situations that we have heard, the thing that the ISPs have had to rely on are the clear law that says, we are not allowed to turn this over unless you can show X, Y or Z. That is very important that that be there.

Mr. SCOTT. I am well over my time limit, but I did want to get in one more point, not really a question. And that is, Mr. Malcolm, you indicated that people don't take these seriously, and I was wondering whether or not we ought to have some advertising like cable TV does to explain to people that stealing cable service is, in fact, a crime. Some advertising to let people know that cyber crime is, in fact, a serious crime so that it will not be taken lightly. I don't know if that is something the Department of Justice could do, but I think that might get the message out a little more directly than waiting for people to have committed serious crimes and then worry about whether they are going to get 2 years, 6 months, 10 years or what.

Mr. MALCOLM. Well, Congressman, as the deputy assistant who oversees the computer crime and intellectual property section, we firmly believe in sending out a message of deterrence. And I will be happy to take your views back to the Department.

Mr. SMITH OF TEXAS. Thank you, Mr. Scott and I will recognize myself now for questions. Actually, both Mr. Coble and Mr. Scott have asked questions that I had intended to, so let me follow up first on Mr. Scott's. Mr. Malcolm, you did a good job of explaining, I think, why we are looking to a good faith standard as opposed to reasonable person standard. Mr. Smith, you had your hand in the air. You gave a good example a while ago. I don't know if you want to add to it or not, and I was going to ask Ms. Koeppen if she wanted to add to that as well.

Mr. Smith, why don't you go on.

Mr. SMITH. What I would urge the Committee to consider is who is in a better position to make a judgment about the immediacy and the reasonableness of a threat? And an ISP employee at 2 o'clock in the morning should be held to a lower standard, law enforcement investigators are the experts on what is an immediate threat and what is a reasonable threat. So I think allowing the ISP to—even a cautious ISP to report a crime or a possible threat to—of death or injury should be the purpose of this legislation rather than to inhibit the reporting of such a threat.

Mr. SMITH OF TEXAS. Okay. Thank you, Mr. Smith.

Ms. Koeppen.

Ms. KOEPPEN. Yes. I would like to add, too, that the scenario that Mr. Davidson described, I mean, we are one of the larger ISPs

in the United States, and it is just not consistent with what our experience has been. We treat requests as requests. We recognize we have the right to say no if we are not satisfied that the statutory conditions are met, and we do require law enforcement to give us a factual basis for the request so that we can make a determination as to whether it is an emergency and meets the requirements of the standard.

And I would—I would echo Mr. Smith's comments about the good faith standard. We believe that is a workable one for providers, and we believe that there is existing precedent in other case law and——

Mr. SMITH OF TEXAS. I just was going to ask you, isn't there precedent as far as a good faith standard goes with some activities by law enforcement?

Ms. KOEPPEN. There is. A law enforcement agent is allowed to act in good faith on a search warrant, even if it later turns out that that search warrant was, in fact, invalid. The evidence collected as a result of that is not subject to suppression. So there is a workable standard that exists in current law today.

Mr. SMITH OF TEXAS. Now, Ms. Koeppen, let me go to another subject, and the same question will be directed toward Mr. Smith, and that is, what is the extent of the problem at Microsoft? What is the extent of the problem, Mr. Smith, with your association members as far as computer crime goes, you know, if you can put a figure on the cost fine. If you can't, we know in general that the problem has doubled in the last year, just from the number of incidences of security breaches, but give us sort of a real-life description of the extent of the problem.

Ms. KOEPPEN. Well, we expend enormous resources in combating this problem. We have to maintain the security of all of the networks that we run. We have a full-time dedicated security incident response center, and when there is an incident, those folks work around the clock to try to determine the source of the problem and come up with a solution, both for our network security and also for customers using our products. So we have to devote tremendous resources to this effort, and we have seen the problem growing. One of the reasons that it is growing so much is that it doesn't take all that much technical expertise anymore to attack a network. Many of these exploits are widely available on Web sites, available for download, you know, point and click and run an exploit against a network. And so the problem has increased tremendously.

Mr. SMITH OF TEXAS. Okay. Mr. Smith, what about your members?

Mr. SMITH. I cannot quantify the problem, but I can say that it is constant and it is not abating. I would also point out that it often originates outside the United States, and in that respect, I would commend the computer crime and intellectual property section's leadership, working with the G-8 and with other countries, to improve the investigation and prosecution of cross border cyber crime, because that is the trend of the future.

Mr. SMITH OF TEXAS. Okay. Thank you. My time is up. I do have a couple more questions which I will get to in a second, but I want

to recognize the gentleman from Ohio, Mr. Chabot, for his questions first.

Mr. CHABOT. Thank you, Mr. Chairman. I want to, first of all, thank you for holding this hearing and then secondly, to apologize for being here a little late. I had some other duties which called. And some of the questions that I was going to ask have already been asked at this point, so I just have one. And I think it is very important to enhance penalties for cyber crimes, especially with heightened awareness of terrorist activities conducted in cyberspace. Not only should we increase the penalties for these crimes, but we should take steps to prevent them from happening to begin with, to the extent possible. I know—and I would ask this question of Ms. Koeppen and Mr. Smith. I know you are going to great lengths to protect your networks, but with technology evolving every day, what steps need to be taken now and in the future? What can be done to upgrade security measures to prevent these crimes from occurring and to protect the private information of consumers?

Ms. KOEPPEN. Well, I think that important thing is the renewed emphasis on security and an understanding that everyone has to secure their connection to the network. We are trying to make that easier to do through our products. We are trying to make it easier for consumers and end users to be able to automatically update the latest security patch and know that they are running the most secure version. But it is really a problem across all networks, because any vulnerability introduced into one network introduces it into all networks, and so I think it is a renewed emphasis by businesses and by consumers on computer security.

Mr. CHABOT. Thank you. Mr. Smith, would you like to comment?

Mr. SMITH. I think you are seeing strong signs of private sector prioritization of this issue at Microsoft and at other companies, including the member companies of the USISPA. I think the Federal Government has an important role to play in being an intelligent consumer of secure products and secure services, and to include as part of its procurement exercises requirements for enhanced security features and enhanced security services. Many of our companies provide top-rate security services, but find it hard in the marketplace to be compensated for that, and we would like that to change.

Mr. CHABOT. Yes, sir.

Mr. DAVIDSON. I just might add, I think that what you are hearing and I think appropriately is that this is an area where the private sector is going to have to lead and appropriately. So there is a role for Government, but it is relatively limited and I think what we are hearing is the market signal from consumers which is extremely important, which is, that consumers won't be able to trust the network and realize the promise of the Internet if their security and privacy isn't protected. I think you are hearing from companies which understand that, which is good.

Mr. CHABOT. Thank you very much. Once again, I would like to commend the Chairman for taking up this very important issue and trying to address it. I yield back the balance of my time.

Mr. SMITH OF TEXAS. Thank you, Mr. Chabot. We are going to give Mr. Goodlatte a chance to get oriented here and recognize Mr. Scott for another question or two, and then go to Mr. Goodlatte.

Mr. SCOTT. Thank you. Ms. Koeppen, if you are asked by law enforcement to provide information, what would you like to do?

Ms. KOEPPEN. I am sorry?

Mr. SCOTT. What would you like to do? What would you like the law to do? Would you like the responsibility of investigating to determine whether or not the request is appropriate, or would you rather, just if the Government asks—just like to comply—my sense is that most ISPs would just like to comply, unless the law requires them to do something else.

Ms. KOEPPEN. Well, Congressman, I think that, first of all, as an ISP, we have privacy to our end customers is a very important part of the service that we provide. Were we not to protect their personal information, people wouldn't be signing up for our service. So we take that commitment to privacy very seriously. This provision is intended to address what we believe are the very rare circumstances where we either come across information or law enforcement comes across information where there is an immediate threat to life or limb and we are able to disclose this information, without delay, to prevent potential deadly harm from happening.

In the case of law enforcement, I imagine law enforcement may come to us one day when they believe we have information. In the case of other Government agencies, though, I think it is more a circumstance where we will go to them, because we have stumbled across something that directly affects their employees or their interests, and they are best situated to respond immediately to the danger or the threat.

Mr. SCOTT. I think we have two different questions. One, if you trip across some information, can you act on it? And another is how you respond to a Government agency asking you for information. I view those as two different questions.

Mr. Davidson.

Mr. DAVIDSON. I think that they very much are and I think that it is companies like Microsoft who are really in a good position to have excellent attorneys and are able to do exactly what we are hearing described, which is to evaluate the requests. I think Mr. Smith, in some ways, has made your point, which is to say the ISPs aren't going to be—don't want to be the ones to have to make that determination all the time that the 2 o'clock network—the network operator at 2 o'clock in the morning who gets this request shouldn't have to, doesn't want to try to evaluate it, and I think probably won't.

And it is not that the good faith exception is the issue here. I think the issue is really what the circumstances are and also who the entities are that can request this information and have it revealed to them. I haven't really heard anything today to say that it really needs to be as broad as the statute reads right now, which is any governmental entity.

Mr. SCOTT. Well, Mr. Malcolm, let me ask you a question and then you can answer. This is just limited to emergencies.

Mr. MALCOLM. That's correct.

Mr. SCOTT. If it were not an emergency, what would you have to do to get the information and what standard would be used?

Mr. MALCOLM. Unless there were another exception that would permit voluntary disclosure, say, such as hacker trespass, then in order to get the information that we are talking about, presuming it is content, one would need to go get a search warrant. Law enforcement would have to go get a search warrant, and if we were talking about a real-time intercept, you would have to get a title III order. But there would be——

Mr. SCOTT. And that would require probable cause?

Mr. MALCOLM. Yes.

Mr. SCOTT. Okay. Did you have another comment?

Mr. MALCOLM. Yes. You know, I guess what strikes me about Mr. Davidson's comment is that these are rare circumstances and that law enforcement is not going to be going about calling ISPs willy nilly in nonemergency situations unless they have a genuine belief that it is an emergency; the information is required immediately, i.e., not enough time to go to a judge for process, and involves a threat to life or limb. And in that circumstance, an ISP will review the information to see to it that the statute is complied with and once they have access to the information, law enforcement doesn't have access to that information, they are in the best position to independently determine whether this threat exists. And so long as they are acting in good faith, there is no problem. They are not going to simply roll over. It is certainly not the experience of law enforcement that they roll over, and we are talking about situations in which urgency is of the utmost importance.

Mr. DAVIDSON. I don't think anybody is disputing that there should be emergency. There should be emergency disclosure provisions. It is a question of how broad they should be. When Congress is faced with this kind of he said/she said situation, there is a thing that I think Congress can do, which is to put a reporting requirement in and try and find out—we have no idea how many requests there are out there. Anecdotal evidence that we have been accumulating, which we would be happy to share as much as we can, indicates that it is happening a lot more. We would urge the Committee to put a reporting requirement——

Mr. SCOTT. Well, there is—Mr. Chairman, there is one safeguard here. If the suggestion is it is an emergency and they get the information that there really wasn't an emergency, I mean, the exclusionary rule would help us out a little bit because you wouldn't be able to use the information in court, I would imagine.

Mr. MALCOLM. Congressman Scott, first of all, if there were not truly an emergency, or at least it did not appear as if there was an emergency, there would be no good—there would be no good faith under those circumstances to justify that.

Mr. DAVIDSON. I am sorry. Nobody would know about it. That is the problem. The subscriber would never know that their sensitive communications, their communications with their doctor or their banker were revealed. No one would ever know. It just disappears into the ether.

Mr. MALCOLM. I would like to stress one more thing, Congressman Scott, which is, the ISPs who are aware of this provision know that this is a voluntary provision. So there is nothing that requires

them, when getting a request from law enforcement, to turn over the information. They are not entitled—they are not required to police for the information, and if it turns out that they don't think that the statute applies or they don't feel like giving the information, law enforcement is stuck getting the process. This is a purely voluntary process.

Mr. SMITH OF TEXAS. Mr. Scott, you have generated a good discussion.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. SMITH OF TEXAS. We will go to the gentleman from Virginia, Mr. Goodlatte, for his questions.

Mr. GOODLATTE. Mr. Chairman, thank you very much, for recognizing me. I apologize for my late arrival. Unfortunately, I had to be in more than one place today, but I do want to strongly commend you for introducing this important legislation, which I am very pleased to cosponsor, and for holding this hearing on the legislation that would increase penalties for cyber crimes, enhanced law enforcement coordination and increase the resources to fight cyber crime. I do have a statement that I would ask be made a part of the record, and I won't—

Mr. SMITH OF TEXAS. Without objection.

Mr. GOODLATTE [continuing]. Read the whole thing. But I will say that as the Chairman of the Congressional Internet Caucus and the House Republican high-tech working group, we have seen an explosion in cyber crime in recent years. Everything from computer hacking to child pornography to Internet gambling, and the Internet has increasingly been used to perpetrate fraud. That seems to be the most prolific thing in terms of criminal activity on the Internet. It becomes a seemingly anonymous vehicle with which people can perpetrate various types of crime, and while we have to be very concerned about promoting the growth of the Internet and protecting the freedoms that the Internet brings to everybody, we have, at the same time, to not allow it to turn into the wild, wild west of the 21st century.

Mr. Chairman, today I am introducing legislation that deals with the problem of creating a uniform standard limiting service provider's liability for content that third parties have stored or placed on their systems. This has become an increasing problem for Internet service providers because of the ubiquitous nature of the Internet and the fact that many States are concerned about the proliferation of crime on the Internet and are passing their own laws to address this problem.

This creates a problem for Internet service providers, because it has the effect of requiring Internet service providers to comply with conflicting and varying legal standards, and it therefore has become increasingly apparent that we need to have one uniform standard dealing with the liability of the online service providers for activities that take place by other people, but on their services. And it is my hope that we can—I am sure this legislation will be referred to your Subcommittee, and it is my hope that we can take a very close look at this issue, perhaps even consider whether or not it can be included in the legislation you have, whether at the Subcommittee or the full Committee level or whatever your desire would be, I would very much like to work with the Committee to

see whether there is a place for this type of provision to set a standard that will help us to better enforce our criminal laws, because we will know who is liable and who is not.

And in that regard, I would just like to ask one question, and that would be of Mr. Smith, who represents an Internet service provider and ask him if he can tell us what kind of difficulties his company has encountered and whether he thinks such a uniform standard would be helpful?

Mr. SMITH. Yes. I am here today on behalf of the U.S. ISP Association, and I can say that our Members would be very interested in reviewing the legislation you have introduced. We know that cooperation between ISPs and law enforcement is absolutely essential to fighting cyber crime, but an impediment to cooperation is ISP's concern about liability for messages or content crossing their networks and stored on their networks.

A secondary concern of ISPs is how to administer slightly different laws. If there is one framework for child pornography and another for fake IDs and a third for cyber gambling, trying to administer that inside the company is very difficult if the standard for intermediary responsibility differs from crime to crime. So a uniform standard would appear to be of great benefit to the ISP industry and provide some uniformity in our practices and further cooperation.

Mr. GOODLATTE. Are you saying it would actually further the cooperation with law enforcement, because you know where you stand, and it is not a matter of trying to avoid your own liability but simply knowing where you stand in that regard and then being free to cooperate with law enforcement with regard to those who are actually perpetrating these crimes?

Mr. SMITH. Clarity in the legal framework will enhance cooperation and enhance the concerns of privacy groups who want to know the precise legal framework in which ISPs and law enforcement interact.

Mr. GOODLATTE. Thank you, Mr. Chairman.

Mr. SMITH OF TEXAS. Thank you, Mr. Goodlatte. Let me follow up on a question that Mr. Coble asked Mr. Malcolm and direct it toward you. He asked you what suggestions you had for improving the legislation. I think I have only got two questions left. They only deal with emergencies, though of different kinds. One to direct to you and one to Mr. Davidson.

The question really that I had is that as you know under current law, you can use trap and trace devices, pen registered devices when there is an emergency situation for up to, I think, 48 hours without getting the requisite court order. Is it my understanding that you think that that should be changed for purposes of this legislation or not?

Mr. MALCOLM. Yes, Mr. Chairman. The trap and trace device, as you know, is an indispensable tool of law enforcement. It also happens to be the least intrusive means of assisting law enforcement in an emergency. In an emergency, the ability to install a pen register or trap and trace device can make the difference between whether or not you avert a disaster or whether or not you actually catch a criminal. The emergency pen register statute, as it is currently constituted, while quite good, there have been matters

brought up since September 11th have shown that there are occasions when it can prove a hindrance and the Department would actually recommend expanding the emergency pen register or pen trap statute, which is section 3125, in two ways: By adding immediate threats to a national security interest, and also ongoing cyber attacks of protected computers. The reason this is needed, Mr. Chairman, is because not all threats to a national security interest are going to involve an immediate threat of danger of death or serious bodily injury, yet attacks on critical infrastructure, such as attacks on computers used by the finance markets, the banking networks, parts of transportation may be of the utmost importance and require proceeding with alacrity.

Similarly, Mr. Chairman, it is often impossible to discern at the outset of a cyber attack whether that attack is going to involve a threat to life and limb or a threat to a critical infrastructure; nonetheless, the ability to get up a trap and trace device can make the difference in determining what the intent of that hacker is and whether or not you catch that hacker.

Mr. SMITH OF TEXAS. Okay. Thank you, Mr. Malcolm. Mr. Davidson, I have a question about emergencies, though of a different kind for you. If you don't give the right answer, I am going to ask Mr. Malcolm to respond.

Mr. DAVIDSON. An incentive to get—

Mr. SMITH OF TEXAS. You seemed to object in your testimony a few minutes ago to disseminating information to other Government agencies to the expanded list of agencies that we have in the bill itself. But in the case, say, of a biological attack, why wouldn't we want to as quickly as possible get to, say, the Centers for Disease Control? In the case of an anthrax, real or imagined attack, why wouldn't we want to be able to contact the Post Office as quickly as possible? Why wouldn't we support expanding the agencies that we would want to share information with as soon as we were aware of the nature of the emergency?

Mr. DAVIDSON. Well, I think as a baseline, these are very sensitive communications we are talking about, people's e-mail, the content of communications, not just the transactional data like pen register. So this can be very sensitive information, and I think that there is—somewhere in between the notion of just law enforcement and the notion of any governmental entity, there may be the right answer that you are looking for. But the problem is that as crafted right now, any governmental entity—really it includes a schoolteacher. It includes librarians potentially. It could include the local dogcatcher. It could include Congressional staffers and we know they will, but it is not clear that in this situation ISPs should be able, upon a request that they believe in good faith says that there is a danger out there of threat to life or limb, should be able to turn that information over to all of those people.

Our belief has been that the current—the way the current law is crafted is the sense that the first place that you should go, if you believe that there is a threat of serious injury or death, is law enforcement. That is the right answer, and I think that Mr. Smith's ISP operator at 2 o'clock in the morning, if he believes that there is a problem, should be going to law enforcement and let law enforcement, who is trained to do this, figure out whether the next

person to call is the CDC or somebody else, and we would be happy to work with the Committee to try and find a way to narrow this, but as drafted right now, really you are talking about literally thousands, perhaps hundreds of thousands, of Government employees who could be shown this sensitive information.

Mr. SMITH OF TEXAS. Okay. Thank you, Mr. Davidson.

Mr. DAVIDSON. I don't know if that was the right answer.

Mr. SMITH OF TEXAS. Mr. Smith, do you want to comment?

Mr. SMITH. Yes. I would like to go back to the starting point, which is this is an emergency. Timing is critical. How much time do you want an ISP to be researching the facts to establish that their position is reasonable? How much time do you want the ISP to be thumbing through a directory, finding a qualified Government agency to report this to as opposed to one that would not be qualified? What you want is a good-faith assessment by the ISP that this is an emergency, that someone's life is in danger, and then get the word out to the Government.

Mr. SMITH OF TEXAS. Mr. Malcolm, we will give you the last word.

Mr. MALCOLM. Well, Mr. Davidson's fear that somehow if an emergency comes up, that the ISP is going to be contacting the local librarian is I believe apocryphal. I believe that, Mr. Chairman, you hit the nail on the head. In a situation of an emergency, law enforcement is going to have an awful lot of scrambling to do. And, for instance, in the case of a bioterrorism attack, it is perfectly reasonable, it is eminently efficient and can be life saving for that ISP to be able to contact FEMA or the CDC or some appropriate law enforcement official. ISP are responsible corporate citizens, and they are going to know who to contact in the event of an emergency. And that is what we are talking about here, emergencies.

Mr. SMITH OF TEXAS. Okay. Thank you, Mr. Malcolm. Thank you all for your excellent testimony. It has been very helpful, very useful, and we will take all of that in consideration as we move forward. Appreciate your being here. And we stand adjourned.

[Whereupon, at 5:15 p.m., the Subcommittee was adjourned.]

A P P E N D I X

MATERIAL SUBMITTED FOR THE HEARING RECORD

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON LEE, A REPRESENTATIVE
IN CONGRESS FROM THE STATE OF TEXAS

Good afternoon. I would like to thank Mr. Chairman and the Ranking Member for convening this hearing today.

The Internet is a social, cultural, commercial, educational, and entertainment global communications system whose purpose legitimately benefits and empowers online users. It lowers the barriers to the creation and the distribution of expressions throughout the world.

Throughout history, governments have overreacted to all forms of communications technologies including the printing press, the telegraph, telephone, post, cinema, radio, television, satellite, and video. Now, the Internet is receiving the same kind of treatment.

But this time, after the tragic events of September 11, government must assure that terrorist acts are not performed via the Internet.

Cyber crime, or computer crime, has become increasingly prevalent in our society, as well as around the world. But in order to effectively combat this we, as lawmakers, must keep in mind our civil liberties.

Among other things, H.R. 3428 would expand law enforcement's arm in fighting cyber crime. It would lower the standard for information sharing in emergencies from "reasonably believes" to a "good faith" standard. The Patriot Act has already included in its body many of the provisions we will hear about today.

The reasons behind this bill focuses on public safety. However, giving up freedom will not give us security.

Secret surveillance and interception of all forms of communications including Internet communications cannot be acceptable in democratic societies. Democratic values are strengths, not weaknesses. We cannot infringe on our rights guaranteed by our Constitution.

Congress must balance the competing interests of law enforcement in detecting and prosecuting terrorists against individual rights to privacy, and not to be subject to unreasonable searches and seizures. However, the events of September 11 have shifted the balance towards law enforcement.

I look forward to the testimony today so we can work together to combat Internet crime, while maintaining our rights to privacy.

PREPARED STATEMENT OF THE HONORABLE BOB GOODLATTE, A REPRESENTATIVE IN
CONGRESS FROM THE STATE OF VIRGINIA

I would like to thank the Chairman for introducing this important legislation and for holding today's hearing. I am pleased to be a cosponsor of this comprehensive legislation to increase penalties for cyber crimes, enhance law enforcement coordination and increase resources to combat cyber crime.

Continued growth in the information technology industry is the key to maintaining and strengthening the competitiveness of the American economy in the 21st century. However, that growth could be stymied by the use of technology mediums, such as the Internet, for criminal activity.

Cyber crime has exploded in recent years. From computer hacking to child pornography and Internet gambling, the Internet has increasingly been used to perpetrate fraud and circumvent the law.

Even more troublesome is the threat of cyber terrorism. Today, the United States is dependent on private sector information and computer networks that make up the

critical information infrastructure. A future terrorist attack won't have to use planes or bombs—it could use keystrokes to target the cyber-systems at the heart of operation and control of our nation's critical infrastructures. Computer networks control our air traffic, telecommunications, the New York Stock Exchange, power grids and hospitals.

Now more than ever, we must promote our national security and prevent crime by ensuring the security, confidentiality and authenticity of electronic networks, information and users. That is why I fully support legislation, such as that introduced by Chairman Smith, to crack down on those individuals who engage in criminal activity in the cyber world.

However, while we must increase the penalties for engaging in cyber crime and increase the resources needed to combat such illegal activity, we must be careful not to extend criminal liability to any Internet service provider based on content supplied or controlled by a third party.

No single issue will have a greater impact on the future of the Internet than the resolution of how the government will regulate conduct and content on the Internet. That is why I am introducing today legislation that would create a uniform standard limiting service providers' liability for content that third parties have stored or placed on their systems.

Criminal statutes regulating online criminal activity have taken varied approaches to the liability of service providers. This has created uncertainty for service providers as they wade through the myriad of criminal statutes and the various standards to which they are held liable. Service providers are expected to choose the correct law, from among many competing jurisdictions, and apply it to each of the millions of activities that occurs daily on their networks.

Instead of focusing on those who initiate or profit from illegal activity, some proposals would hold service providers criminally liable for the conduct, activities, and decisions of third parties who use their services. Under many of these proposals, culpability would arise regardless of whether a service provider has any relationship with the user or the offending site, or intends to facilitate the illegal activity. These approaches will not work. There are more effective and responsible ways to combat illegal conduct on the Internet. Instead of targeting service providers, solutions should focus on those who engage in unlawful activity.

As we move forward in consideration of the Cyber Security Enhancement Act, I look forward to the opportunity to work with the Chairman to obtain his support for the legislation I am introducing today, both on its own merits and in the context of this comprehensive cyber crime legislation.

Thank you again Mr. Chairman for holding this important hearing and for your sponsorship of this much needed legislation to combat cyber crime.



February 12, 2002

The Honorable Lamar Smith
Chairman, Subcommittee on Crime
Judiciary Committee
U.S. House of Representatives
207 Cannon House Office Building
Washington, DC 20515

Dear Chairman Smith:

On behalf of the Information Technology Association of America (ITAA), I am writing you today to voice support for the Cyber Security Enhancement Act of 2001 (H.R. 3482), which you and House Science Committee Chairman, Sherwood Boehlert, introduced in December 2001. I urge the U.S. House of Representatives to pass this measure in early 2002.

H.R. 3482 is an important piece of legislation that ITAA believes is important for strengthening guidelines on sentencing people who are convicted of cyber crimes. As you know, American security, including security against cyber-crime and cyber-terrorism, is critical to remaining a global leader. We urge the U.S. Congress to act now and pass H.R. 3482 and companion legislation in the Senate.

We also look forward to continuing to work with you and other House leaders to substantially increase funding to secure government information systems at the federal and state level, and, to remove barriers to information sharing between government and industry to enhance the analysis, prevention and detection of attacks on U.S. critical infrastructure.

Thanks again for your continued leadership on these issues.

Sincerely yours,

Harris N. Miller
President

Cc: The Honorable Sherwood Boehlert

Information Technology Association of America

1401 Wilson Blvd., Suite 1100, Arlington, VA 22209 - 2318 ■ Phone: (703) 522-5055 Fax: (703) 525-2279



February 26, 2002

The Honorable Lamar Smith
 Chairman, Subcommittee on Crime
 Committee on the Judiciary
 U.S. House of Representatives
 Washington, DC 20515

Dear Chairman Smith:

The Interactive Digital Software Association (IDSA) would like to express our support for H.R. 3482, "The Cyber Security Enhancement Act of 2001," as it was voted out of the Crime subcommittee on February 26, 2002. We also want to express our thanks to you, and the other members of the subcommittee, for your leadership and hard work to increase the penalties for those whom engage in cybercrime.

IDSA is the U.S. association exclusively dedicated to serving the business & public affairs needs of companies that publish video & computer games for consoles, personal computers & the Internet. IDSA members collectively account for nearly 90 percent of the \$6.3 billion in entertainment software sold in the U.S. in 2001, and billions more in export sales of U.S.-made entertainment software. Our members create and distribute interactive game software in digital format, making it susceptible to electronic theft, unauthorized reproduction, mass duplication and Internet transmission. Accordingly, the security and protection of digital content on the Internet is extremely important to our member companies.

Thus, one of our highest priorities is ensuring the protection of copyrighted material owned by our member companies, especially on the Internet. That objective has become more and more challenging over the past few years as the world has quickly moved into the digital age and governments have struggled to keep up with the enhanced piracy opportunities presented by this new technology. In addition, as our members increasingly embrace on-line video game business models, with the wider introduction of broadband, H.R. 3482's increased penalties for hacking and enhanced sentencing flexibility is a huge plus.

We hope the Committee will continue its efforts to crack down on cybercrime, which compromises the business opportunities for our industry and many others, and defend the safety of the Internet by passing this important legislation.

Sincerely,

A handwritten signature in dark ink, appearing to read 'Doug Lowenstein', is positioned above the typed name.

Doug Lowenstein
 President,
 Interactive Digital Software Association

ELECTRONIC PRIVACY INFORMATION CENTER



February 26, 2002

BY MAIL & FAX

The Honorable Lamar Smith, Chairman
Sub-committee on Crime
Committee on Judiciary, United States House of Representatives
2231 Rayburn House Office Building
Washington, DC 20515-4321
Fax: 202.225.8628

The Honorable Robert C. Scott, Ranking Member
Sub-committee on Crime
Committee on Judiciary, United States House of Representatives
2464 Rayburn House Office Building
Washington, DC 20515-4603
Fax: 202.225.8354

1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA
+1 202 463 1140 (tel)
+1 202 463 1248 (fax)
www.epic.org

Re: H.R. 3482 "The Cyber Security Enhancement Act of 2002"

Dear Representatives Smith and Scott,

We are writing to comment on H.R. 3482 "The Cyber Security Enhancement Act of 2002" (CSEA) that may be considered by the Subcommittee this week. We request that this letter be placed on the hearing record. Several sections in Title I of CSEA raise important questions about the appropriate Congressional response to the problem of cyber crime. Section 102 in particular allows for a significant expansion of enforcement authority without corresponding judicial oversight. We recommend that your Committee take the opportunity make changes in the bill so that it is consistent with current privacy law and with our constitutional limitations on government investigative power.

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C. that seeks to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. For over a decade we have reviewed proposals for information system security in the federal government, testified on the subject at House and Senate hearings, made recommendations for changes, and pursued litigation where appropriate. EPIC Executive Director Marc Rotenberg has testified before Congress regarding computer crime on several occasions.

¹ As per the amendment proposed on February 12, 2002, available at http://www.techlawjournal.com/cong107/cybersecurity/hr3482_20020214.asp.

As you are aware, our country has become increasingly dependent on high-tech infrastructure for everything from power and communications to transportation and national defense. Computers and the Internet are also becoming more accessible to broader segments of the population who rely on them for a wide range of transactions.² Information system security is therefore a serious problem that demands carefully calibrated action from the government. Punishing fraud, developing effective deterrents to criminal behavior, coordinating enforcement activity are all measures that will improve our security. But any effort to protect our security remains should be appropriately tailored to the problem identified and should be consistent with our constitutional values. Clearly, well established safeguards and constitutional protections should not be diminished simply because the criminal might operate in the "virtual" world.

Specifically, we draw your attention to the following sections of CSEA that require further consideration.

Section 101: Sentencing Guidelines

Section 101 directs the United States Sentencing Commission (USSC) to amend sentencing guidelines related to cyber crime. We support the view that the penalties for cyber crime should closely follow their counterparts for crimes in the physical world. Particular attention needs to be placed on the harm caused by cyber crime and in creating effective deterrents and remedies to protect consumers and other affected parties. We welcome §101(6), which requires the USSC to take into account the violation of individuals privacy rights in drafting sentencing guidelines. The USSC should draft guidelines that are fair, equitable and appropriately tailored to the extent of the harm caused.

We also urge Congress to consider drafting parallel laws that would make software companies and other information technology providers legally accountable for weak or lax security. The notion that a company can produce a consumer product that is systemically flawed, and not be liable, appears to only hold true in the information technology industry.

Section 102: Emergency Disclosure

Section 102 is a major departure from existing privacy protections in the law. This section allows law enforcement authorities and other governmental entities to circumvent the legal protections to access the content of communications, and it provides no scope for oversight or governmental accountability. The USA PATRIOT Act of 2001 already allows communication service providers to disclose the content of their customer's communications to law enforcement authorities if the provider

² A Nation Online, Department of Commerce Report, available at <http://www.esa.doc.gov/508/esa/nationonline.htm>.

“reasonably believed” that the information was regarding an “emergency involving immediate danger of death or serious physical injury to any person” (18 U.S.C. 2702(b)(6)(e)).

We note that the PATRIOT Act enacted sweeping changes in computer crime and government surveillance statutes without proper deliberation and despite law enforcement and intelligence agencies already possessing broad authority to conduct investigations of suspected terrorist activity. Section 102 of CSEA seeks to further modify a section of the law despite any clear or convincing demonstration of need.

Section 102 departs from the PATRIOT Act in three key respects:

- The information can be divulged to *any* governmental entity – from school principals to the Center for Disease Control. Under current law only law enforcement authorities are authorized to receive the information.
- The information can be turned over by the communications providers merely on a “good faith” standard rather than the more responsible “reasonable belief” standard. This lax standard will endanger users’ privacy because providers can rely on the side of increased disclosure without taking into interest their customers’ rights.
- The proposed standard for the content of the communications is no longer an “immediate danger” to life or limb, but simply a vague and expansive “danger.”

Allowing information to be disclosed to any government entity is not only a great risk to personal privacy, but is plainly a poor security strategy. To permit broad access to sensitive information to so many entities could easily create new security risks. A specific agency designated to handle such disclosures can provide an important information clearinghouse function and should be equipped to route critical information expediently to the appropriate agency. Most government entities would otherwise have trouble sorting through a flood of information. The CDC for instance ignored an e-mail message from a Canadian team that conducted a critical study on the Anthrax mail delivery model for two months, because the person in charge was inundated with messages.³

Limiting disclosure to one entity might also restrict the misuse of the law in practice, where enforcement authorities *approach* the communications providers for emergency disclosures of content. The law specifically provides that under those conditions the information collection requires proper judicial authority. There is a highly evolved judicial practice in granting access under time-sensitive conditions that law enforcement can avail if appropriate. The emergency disclosure provision, if

³ Chad Terhune, Canadian Officials Did Research On Anthrax Before U.S. Attacks, Wall Street Journal, December 12, 2001.

it has any utility, provides an avenue for communications providers to disclose information that they might have inadvertently come across. Such disclosures should at least be limited to when the provider *reasonably* believes that there is an *immediate* danger. Providers should not become an agent of law enforcement by routinely turning over their customer's private communications under a weak "good faith" and any "danger" standard. The provider's liability for such disclosures ought to be dealt with elsewhere in the law if necessary without changing the standard.

There is also an urgent need for Congress to create proper public and judicial oversight for the use emergency disclosure procedures. Because there is no record or audit trail for such requests some of the public commentators are forced to rely on suppositions and anecdotal evidence. Congress must also draft a provision that notice of such disclosure must be provided to the suspect at an appropriate juncture, following the law with respect to wiretaps.

Section 106: Increased penalties under 1030(c)

Section 106 adds a new sub-part to the penalties under 18 U.S.C. 1030(c) introducing fines and potential life sentences for offenders who either knowingly or recklessly attempt to or cause death to any person. Section 106 also provides for fines and prison terms up to 20 years for offenders who knowingly or recklessly attempt to or cause serious bodily injury. Clearly offenders who use computer technology to kill or seriously injure others ought to be punished for their crime and that punishment should be consistent with penalties for crimes perpetrated through other means. However, it is not clear why the use of a computer as an instrumentality should be the basis for elevated sentencing. Congress should instruct the Sentencing Commission to research and report on sentencing guidelines that will ensure that computer criminals are punished appropriately for their crimes. Recklessness, for example, is not usually treated as rising to a sufficient criminal level of intent to warrant such prison terms.

Section 107: Provider Assistance

Section 107 inappropriately attempts to create a new information collection tool for law enforcement. Under current law a court order or a certification is needed to access private communications. Section 107 will allow a government entity's "statutory authority," presumably derived from §102 of this title, to compel disclosure of information. This circumvents existing legal protections. Section 107 also provides for civil penalties for providers who choose to protect their customer's privacy.

Section 108: Emergencies

Section 108 modifies the pen register and trap and trace device standard so that they can be installed without a court order if there is an "immediate threat" to "a national security interest" or when there is an "on-going attack" on a "protected

computer.” These conditions are overly broad – any number of things might be construed as a national security interest and a protected computer includes any computer used in interstate commerce. The threshold for obtaining a pen register or trap and trace device is already low and covers instances where serious harm justifies emergency installation without court order. At least the statutory language for §108 must track the language used for emergency installation of such devices to combat organized crime. An order authorizing the installation and use of such devices must also be thought to be obtainable with “due diligence.” In any event emergency installation must be certified in 48 hours so there is reason for law enforcement to act correctly in the first instance, but the absence of such language might encourage frivolous or temporary use of such devices.

Section 109: Protecting Privacy

Section 109 strikes the lowered penalties for certain first time offenses who intercept private communications from the penalties laid out under 18 U.S.C. 2511(4)(b). Section 109 also increases the penalties for unlawful access to stored communications for first-time offenders from one year to five, and from two years to ten years for subsequent offenses under 18 U.S.C. 2701(b).

Title II: Office of Science & Technology (OST)

The National Institute of Justice was created to encourage partnership and information sharing between various local and federal enforcement authorities. While there are no clear civil liberties implications in creating a separate entity, there hasn't been sufficient debate to illustrate the need for such an entity. We also believe that § 202(b)(2), which creates an exemption for the OST's public-private Advisory Groups from the Federal Advisory Committee Act, is inappropriate because it restricts public access to the Advisory Group's deliberations.

Recommendations

Section 101: The Sentencing Commission should review sentencing guidelines for cyber crime to make them consistent with guidelines for other criminal activity. There should be a provision that makes information technology producers liable for weak security in their products.

Section 102: Strike §102 or amend proposal to ensure that emergency disclosures can only be made to a narrow class of government entities. Additionally, create a means for public and judicial oversight of emergency disclosure activities along with creating a notice provision for suspects.

Section 106: Criminals using computers should receive penalties commensurate with penalties for crimes perpetrated through other means – the use of a computer as an instrumentality should not be the basis for

elevated sentencing. We recommend reviewing the penalties, particularly for reckless behavior, with a view to correct any disproportionate treatment of computer crimes.

Section 107: Strike §107 or at least strike the provision for civil penalties for communication providers who choose to protect their customer's private communications.

Section 108: Strike §108 or else craft a narrower class of activities where emergency installation of pen register or trap and trace devices is permissible. Also modify language so that in the event of an emergency installation, the enforcement authorities should believe that, with due diligence, the installation will receive court permission.

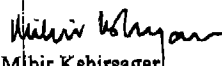
Section 109: Review the current enforcement of the provision in section 2701(b) before further increases in the proposed punishment. The Transactional Records Access Clearinghouse offers extensive information about the current enforcement of the Computer Fraud and Abuse Act.⁴

Title II: Do not make OST Advisory Groups exempt from Federal Advisory Committee Act in § 202(b)(2)

We appreciate your consideration of our views. We would be pleased to meet with you or your staff if you have any questions.

Sincerely yours,


Marc Rotenberg
Executive Director


Mihir Kshirsagar
IPIOP Policy Fellow

⁴ <http://trac.syr.edu>.



WASHINGTON NATIONAL OFFICE
 Laura W. Murphy
 Director

122 Maryland Avenue, NE Washington, D.C. 20002

(202) 544-1681 Fax (202) 546-0738

February 12, 2002

The Honorable Lamar Smith, Chairman
 Crime Sub-Committee of the House Judiciary Committee
 207 Cannon House Office Building
 Washington, DC 20515-4321

The Honorable Bobby Scott, Ranking Member
 Crime Sub-Committee of the House Judiciary Committee
 476 Russell Senate Office Building
 2464 Rayburn House Office Building
 Washington, DC 20515-4603

Re: H.R. 3482 "The Security Enhancement Act of 2001"

Dear Representatives Smith and Scott,

We are writing in regards to H.R. 3482 "The Cyber Security Enhancement Act of 2001 (CSEA)." Overall the bill does not pose serious civil liberties concerns, however, we recommend some slight modifications, which will protect the privacy rights of Internet users.

Section 101 – Amend Directive to Sentencing Commission

Section 101 directs that the United States Sentencing Commission "...shall amend the Federal Sentencing Guidelines and, if appropriate, promulgate guidelines or policy statements or amend existing policy statements." This directive appears to mandate that the United States Sentencing Commission must amend the guidelines, even if amendment is not necessary or appropriate.

The ACLU is concerned that the USSC have the necessary flexibility to determine sentences that are fair. We oppose a directive that takes away this flexibility. A number of the provisions listed in Section 101 are already covered by current guidelines so further enhancement may be unnecessary. See USSC Guidelines 2B1.1 (Nov. 2001). We recommend striking the word "amend" to "review," thereby requiring that the USSC review the guidelines with the detailed factors in mind without mandating an increased penalty.

Section 102 – Strike this provision or provide significant protections against abuses

The government should obtain a warrant based on probable cause before obtaining the contents of individuals' e-mail or other electronic communications. The USA PATRIOT Act included a narrow "emergency exception" to this rule. Internet service providers are permitted to divulge the contents of an e-mail or electronic communication to law enforcement agencies if the "provider reasonably believes that an emergency involving immediate danger of

death or serious physical injury to any person requires disclosure of the information without delay." 18 USC s. 2702(b)(6)(C)

Section 102 of the CSEA would expand this narrow exception in two ways: 1) it allows service providers to disclose the contents of personal communications to *any* local, state, or federal government entity (not just a law enforcement agency); and 2) it allows service providers discretion to disclose information so long as they have a "good faith" belief that there is a danger of death or serious physical injury.

First, the emergency exception included in the USA PATRIOT Act was rooted in the rationale that law enforcement should be able to protect people from imminent physical harm or death. Section 102 goes well beyond the purpose of public safety and allows service providers to disclose e-mails and other personal information to any government entity – at the federal, state, and local level. There is no justification for expanding this exception to every government entity across the country. Law enforcement agencies have primary responsibility for public safety and the "emergency exception" should remain limited to law enforcement. Service providers should not be in the position of determining what other agencies should or should not have access to this private information. If law enforcement needs to share information with other agencies, it should decide when that is appropriate, not the ISPs.

Second, under the USA PATRIOT Act, service providers may only disclose the contents of electronic communications with law enforcement agencies if they "reasonably believe" there is an emergency that involves immediate death or serious injury. Section 102 would eliminate the objective "reasonableness" standard and allow service providers to disclose information based on a subjective "good faith" belief that an individual is in danger. Under this subjective standard, providers would have wide discretion to divulge the contents of personal communications to any number of government agencies if they simply believed – no matter how unfounded – that the disclosure was necessary to prevent death or injury.

We understand that service providers may have concerns about their legal liability for disclosures. However, this provision conflates the standard for disclosure with the standard for determining liability. If Congress wants to afford the ISPs a good faith exception for liability purposes it should expand liability available under 17 U.S.C. sec. 2707. This is a separate issue from determining the appropriate standard as to when service providers should release information. Without an objective reasonableness standard, there would be no deterrent for service providers to go beyond the limits of the law.

Finally, under Section 102, these disclosures would take place without any oversight whatsoever. This provision creates the possibility that law enforcement will abuse its power and avoid the requirements of 18 U.S.C. sec. 2702 by seeking to get information from the service provider by claiming to have reason to believe that there is an emergency that involves immediate death or serious injury, thereby evading any requirement to obtain a warrant.

The purpose of obtaining a warrant or court order is to ensure that law enforcement or other executive branch agencies are not abusing their authority or engaging in unreasonable searches and seizures. Section 102 fails to include even the most basic check and balance on the disclosure of personal communications. There is no notice to a court, a federal agency, or individuals themselves that personal communications have been disclosed to the government. There is no review – either before or after the disclosure – of whether the disclosure was justified in the first place. Under this provision, service providers could disclose information to a range of government agencies in secret – without any type of review or notice. Even the USA PATRIOT Act requires reporting to the courts when law enforcement utilizes Carnivore, a means of intercepting electronic communication.

This provision greatly undermines our privacy by failing to limit the "emergency exception" to the agency responsible for public safety; eliminating the objective "reasonableness" standard; failing to provide any checks and balances on disclosures of personal information; and failing to establish penalties that would act as a deterrent to unlawful disclosures of personal information.

The USA PATRIOT Act lowered the standard necessary for the government to obtain highly private information. See USA PATRIOT Act sections 201, 202, 209, 210 and 217. It also authorized the broad sharing of information between federal law enforcement agencies. See USA PATRIOT Act Sections 202, 701 and 901. We are very concerned that the Congress would expand this already broad authority at this time. There is a real concern that highly private information could be misused and we believe that the Congress should ascertain how the recent changes impact personal privacy before continuing to go down the road of further information sharing.

Sincerely,

Laura Murphy, Director

Rachel King
Legislative Counsel

Katie Corrigan
Legislative Counsel

Cc: House Judiciary Committee

UNITED STATES SENTENCING COMMISSION
ONE COLUMBUS CIRCLE, N.E.
SUITE 2-500, SOUTH LOBBY
WASHINGTON, D.C. 20002-8002
(202) 502-4500
FAX (202) 502-4699



February 11, 2002

The Honorable Lamar S. Smith
Chairman, Subcommittee on Crime
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Robert Scott
Ranking Member, Subcommittee on Crime
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

Re: H.R. 3482 Cyber Security Enhancement Act of 2001

Dear Mr. Chairman:

The United States Sentencing Commission is providing the following comments regarding H.R. 3482, the Cyber Security Enhancement Act of 2001, and requests that these comments be made part of the hearing record. These comments are limited to the proposed directive to the Commission set forth in section 101 of the bill. Section 101 would direct the Commission to review and amend, if appropriate, the federal sentencing guidelines pertaining to offenses covered by section 1030 of title 18, United States Code, and would require the Commission to consider several enumerated factors.

The Commission shares Congress's concern over computer crime, particularly as such offenses relate to our national defense and security. If in Congress's judgment a directive relating to section 1030 offenses is appropriate, the proposed directive as currently drafted by the Subcommittee provides the Commission sufficient flexibility to exercise its judgment and expertise in sentencing policy as envisioned by Congress and set forth in the Sentencing Reform Act of 1984. We would therefore not favor revision aimed at making the directive more specific and less discretionary.

The Commission has demonstrated its ability to address new sophisticated high technology crimes like those covered by the proposed directive, having recently passed amendments relating to electronic copyright infringement, identity theft, digital counterfeiting, and sexual offenses using the computer. In addition, last year the Commission passed an amendment, effective November 1, 2001, that significantly increased penalties for certain nuclear, chemical, and biological weapons offenses. Close collaboration with the Department

through its *ex officio* commissioner has been instrumental in our efforts in these areas.

With respect to the specifics of the proposed directive, there are a number of guideline provisions currently in effect that may be relevant to Congress's consideration of the bill. After studying economic crimes over several years, the Commission promulgated a comprehensive economic crime package that became effective November 1, 2001, that substantially increased penalties for mid and large scale economic crimes, including computer crime offenses covered by section 1030 of title 18, United States Code.

As a result of the recent amendment, USSG §2B1.1, which applies to computer crime offenses, bases the sentence enhancement for "loss" on the greater of actual loss or intended loss. *See* Application Note 2(A) of §2B1.1. Moreover, in a case involving unlawfully accessing or exceeding authorized access to a "protected computer" as defined in 18 U.S.C. § 1030(e)(2), the guidelines require that actual loss include reasonable costs to the victim of conducting a damage assessment, restoring the system and data to their condition prior to the offense, and any lost revenue due to interruption of service. *See* Application Note 2(A)(v)(III) of §2B1.1.

In sentencing computer crime offenses, the guidelines also require consideration of the level of sophistication and planning involved in the offense. The guidelines require a sentence increase of at least two levels (an approximate 25 percent increase), with a minimum offense level of 12, when the offense involves sophisticated means. *See* §2B1.1(b)(8)(C). Under USSG §3B1.3, the guidelines also require a two level sentencing enhancement if the defendant abused a position of public or private trust or used a special skill in a manner that significantly facilitated the commission or concealment of the offense.

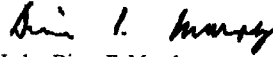
The guidelines require sentence increases for other types of offense conduct that may be involved in a computer crime offense. For example, the guidelines require a two level increase in sentence if the offense involved more than ten but less than 50 victims, and a four level increase in sentence if the offense involved fifty or more victims. *See* §2B1.1(b)(2)(A)(i) and (B). If the offense involved the conscious or reckless risk of death or serious bodily injury, the guidelines require a sentence increase of two levels, with a minimum offense level of level 14. *See* §2B1.1(b)(11).

Finally, the guidelines contain a number of departure provisions that enable a court to sentence above the applicable guideline range in appropriate cases, including if death resulted (USSG §5K2.1), significant physical injury resulted (USSG §5K2.2), or a victim or victims suffered psychological injury much more serious than that normally resulting from commission of the offense (USSG §5K2.3). The court also may increase the sentence above the authorized guideline range if the offense caused property damage or loss not taken into account within the guidelines (USSG §5K2.5) or the defendant's conduct resulted in a significant disruption of a governmental function (USSG §5K2.7).

In addition to these existing provisions, the Commission currently is working on responding to the recently enacted USA PATRIOT Act, Pub. L. 107-56. The Commission is mindful of the increases in statutory maximum penalties provided by the Act and, like it does for all legislative increases in statutory maximum penalties, is carefully studying what amendments to the guidelines may be necessary as a result. We expect to submit an amendment to Congress on May 1, 2002.

The Commission shares Congress's concerns about computer crime and will continue to work closely with Congress and others as appropriate on issues that affect our national security. I hope that you find this information helpful to your consideration of the proposed bill, and please contact us if we can be of any further assistance.

Sincerely,

A handwritten signature in black ink, appearing to read "Diana E. Murphy".

Judge Diana E. Murphy
Chair



1250 Eye Street, NW Suite 200
Washington, DC 20005
202-737-8888 www.itic.org

CHAIRMAN
Tom Green
Dell

PAST CHAIRMAN
Marshall Phelps
IBM

OFFICERS

Rhett Dawson
President
Kathryn Hauser
Senior Vice President
Ralph Hellman
Senior Vice President
Helga Sayadian
Vice President

February 12, 2002

The Honorable Lamar Smith
Chairman, Subcommittee on Crime
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Smith:

The Information Technology Industry Council (ITI) wishes to express our strong support for H.R. 3482, The Cyber Security Enhancement Act. The security of the Internet and the interconnected networks upon which it runs is of paramount importance to the information technology (IT) industry. This bill contributes to the security of the Internet, and Internet users, in several important ways.

Cyber-crimes perpetrated by hackers can disable critical information systems, cost our economy billions of dollars and diminish citizens' confidence to use the Internet safely. Despite industry-wide efforts to improve computer security, the frequency of these crimes has grown as more people experience the Internet. H.R. 3482 allows for greater consideration of the sophistication and intent of an attack when sentencing a convicted cyber-criminal. This change will allow the sentences imposed on these criminals to more adequately reflect the seriousness of these crimes.

H.R. 3482 also incorporates important conforming amendments to the U.S.A Patriot Act passed last year. This bill would allow greater information sharing between communications providers and government agencies beyond law enforcement, as well as protecting providers against liability in assisting law enforcement under new computer trespassing laws within the U.S.A. Patriot Act. These are important provisions that remove obstacles to information sharing between the public and private sectors to strengthen Internet security.

This bill authorizes the National Infrastructure Protection Center (NIPC) to serve as the focal point for critical infrastructure attacks. The NIPC is a vital component of critical infrastructure protection and we strongly support its authorization. This bill also establishes the Office of Science and Technology (OST) outside the National Institute of Justice to accord technology the important position it deserves in current law enforcement activities.

We hope the Committee will demonstrate its commitment to Internet security by quickly approving this important legislation.

Sincerely,

Rhett Dawson
President

The association of leading IT companies
Agilent • Amazon.com • AOL Time Warner • Apple • Canon USA • Cisco • Compaq • Corning • Dell • Eastman Kodak
EMC Corporation • Hewlett Packard • IBM • Intel • Lexmark • Microsoft • Motorola • National Semiconductor • NCR
Panasonic • SGI • Siebel Systems • Siemens Corporation • Sony • StorageTek • Symbol Technologies • Tektronix • Unisys

PREPARED STATEMENT OF STEPHEN E. CROSS

Introduction

Mr. Chairman and Members of the House Judiciary Subcommittee on Crime:

My name is Steve Cross. I am the director of the Software Engineering Institute (SEI) at Carnegie Mellon University. The SEI is the home of the CERT® Coordination Center (CERT/CC) and CERT Analysis Center. I appreciate the opportunity to provide testimony to your subcommittee. I will give you some background on the CERT Centers, describe the trends we have observed while responding to computer security incidents on the Internet, which HR 3482 addresses in part, and discuss further essential steps that I believe can be taken to address the problems we see today and those we can expect to see in the future.

The CERT® Coordination Center (CERT/CC) is part of the Survivable Systems Initiative of the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. The CERT/CC was established in 1988, after an Internet "worm" stopped 10% of the computers connected to the Internet. This program--the first Internet security incident to make headline news--was the wake-up call for network security. In response, the CERT/CC was established at the SEI. Its charter was to work with the Internet community to respond to computer security events, raise awareness of computer security issues, and work with technology producers to resolve vulnerabilities. While continuing to respond to incidents, the CERT/CC provides training, investigates tools and techniques that enable typical users and administrators to effectively protect systems from damage caused by intruders, conducts research leading to increased security of the Internet, and serves as a model to others establishing incident response teams. The CERT/CC is recognized by both government and industry as a neutral, authoritative source of information assurance information and expertise. More details about our work are attached to the end of this testimony (see *Meet the CERT Coordination Center*).

In the first full year of operation, 1989, the CERT/CC responded to 132 computer security incidents. In 2001, the staff responded to more than 50,000 incidents. In total, the CERT/CC staff has handled well over 100,000 incidents and analyzed more than 5,000 computer vulnerabilities. This testimony is based on that broad experience and on the research and analysis under way at our analysis center.

Increasing Risk

Government, commercial, and educational organizations depend on computers to such an extent that day-to-day operations are significantly hindered when the computers are "down." Currently many of the day-to-day operations depend upon connections to the Internet and other interconnected networks, and new connections are continuously being made. The Internet Domain Survey (<http://www.isc.org/ds/>) reports that the Internet grew from 72 million computers in January 2000 to 109.5 million in January 2001; an addition 16.3 million had connected by July 2001, the date of the last survey.

Computers have become such an integral part of American government and business that computer-related risks cannot be separated from general safety, health, business, and privacy risks. Valuable government and business assets are now at risk over the Internet and other information infrastructures. For example, citizen and personnel information may be exposed to intruders. Public safety and health services that are conducted over the networks can be disrupted. Financial data, intellectual property, and strategic plans may be at risk. The widespread use of databases leaves the privacy of individuals at risk. Increased use of computers in safety-critical applications, including the storage and processing of medical records data,

increases the chance that accidents or attacks on computer systems can cost people their lives.

Today there is rapid movement toward increased use of interconnected networks for a broad range of activities, including commerce, education, entertainment, operation of government, and supporting the delivery of safety, health, and other human services. Although this trend promises many benefits, it also poses many risks. Techniques that have worked in the past for securing systems are not effective in the current world of unbounded networks, mobile computing, distributed applications, and dynamic computing. It is easy to exploit the many security holes in our networks and in the software commonly used in conjunction with it; and it is easy to disguise or hide the true origin and identity of the people doing the exploiting. Many of our information systems are easily accessible to anyone with a computer and a network connection. Individuals and organizations worldwide can reach any point on the network without regard to national or geographic boundaries.

In short, interconnections are rapidly increasing, and cyber intruders are using the connectivity to exploit vulnerabilities in systems, compromise information, or launch denial-of-service attacks.

Attack Strategies Illustrating Internet Vulnerabilities

Some attacks are intended to harass a site and deny it the ability to transact business on the Internet. Other attacks enable intruders to gain privileged access to a system so that it effectively belongs to them. With their unauthorized privileges, they can, for example, use the system as a launch platform for attacks on other sites or as one node in an attack using distributed-system intruder tools. Still other attacks are designed to reveal sensitive information, such as passwords or trade secrets. We describe sample attack strategies below. Our descriptions are neither theoretical nor abstract; rather, they present, at a high level, actual attacks reported regularly to the CERT Coordination Center.¹

Use of Distributed System Intruder Tools

Distributed systems based on the client/server model have become increasingly common. Over the past two years, the CERT/CC has seen an increase in the development and use of distributed sniffers, scanners, and denial-of-service tools. Attacks using these tools can involve a large number of sites simultaneously and be focused to attack one or more victim hosts or networks.

Damaged systems include those used in the attack as well as the targeted victim. For the victim, the impact can be extensive. For example, in a denial-of-service attack using distributed technology, the attacked system observes simultaneous attacks from all the nodes at once—flooding the network normally used to communicate and trace the attacks and preventing any legitimate traffic from traversing the network.

The processes for discovering vulnerable sites, compromising them, installing daemons (programs used in the attack), and concealing the intrusion are largely automated, with each step being performed in “batch” mode against many machines in one “session.” Daemons have been discovered on a variety of operating systems with varying levels of security and system management.

¹All the attacks mentioned in this section are described in CERT advisories, published online by the CERT Coordination Center, Pittsburgh, PA, and available from <http://www.cert.org/>

Planning and coordination before an attack are critical to ensuring adequate response when the attack is in progress. Since the attack methodology is complex and there is no single-point solution or "silver bullet," resolution and restoration of systems may be time-consuming. The bottom line is that an organization's systems may be subject at any time to distributed attacks that are extremely difficult to defend against or trace.

Although an organization may be able to "harden" its own systems to help prevent implantation of the daemon portion of a distributed attack tool, there is essentially nothing a site can do with currently available technology to prevent becoming a victim of, for example, a coordinated network flood. The impact upon the site and its operations is dictated by the (in)security of other sites and the ability of a remote attacker to implant the tools and, subsequently, to control and direct multiple systems worldwide to launch an attack. The result may be reduced or absent network connectivity for extended periods of time, possibly days or even weeks depending upon the number of sites attacking and the number of possible attack networks that could be activated in parallel or sequentially.

Coordinated attacks across national boundaries have occurred. The tools and attacks demonstrate that a network that optimizes its technology for speed and reliability at the expense of security may experience neither speed nor reliability, as intruders abuse the network or block its services. Intruder technology is evolving, and future tools may be more difficult to defeat.

Web-Specific Attacks

The CERT/CC has published a number of security alerts about web-related technology including several regarding *cross-site scripting*. In this attack, what users receive from a web site may not be what the operators of that site meant to send. Attackers put malicious code into otherwise legitimate HTML code so that if users click on a specially designed link, they may receive bad data, unwanted pictures, and programs (malicious scripts) to compromise their data. The attackers can capture passwords and other information the users believe is protected, and the attackers may be able to view protected parts of the users' network, such as an intranet.

The problem is not with web browsers themselves but with how dynamic web pages are constructed (*dynamic* means they are constructed "on the fly" in response to user input) and how data entering and leaving web sites is validated. "Validate" means ensuring no unintended characters are sent back to the client. The attack is possible because web browsers have the capability to interpret scripts embedded in web pages downloaded from a web server. Web browsers are usually installed with this capability turned on by default. The user can unknowingly download the script when visiting a seemingly safe site and completing an interactive form or querying a database; following untrustworthy links in web pages, email, or newsgroups; and viewing dynamically generated web pages. The malicious script then runs on the user's browser. Although attackers have been able to inject malicious code for a long time, the cross-site scripting attack is significant because users can acquire malicious code from legitimate, typically trustworthy sites; avoiding questionable sites is no longer adequate protection.

Most solutions require action from a broad community of web page developers and web site administrators. They must ensure that their web pages are encoded in a way that neutralizes malicious code, apply patches developed by vendors, and filter all data that enters and leaves web servers. In the meantime, users can gain some protection by turning off certain features of

their web browsers, limiting the functionality they may be accustomed to having. They cannot fully protect themselves nor easily identify an attack.

The World Wide Web is a young and still immature technology. Until it is “hardened” for safe, effective use, it will continue to be vulnerable to security compromises--and online companies and customers alike will continue to be concerned about the integrity and privacy of information that must be exchanged if they are to do business on the web.

SYN Attacks: Denial of Service

A *SYN attack* is an attack against a computer that provides service to customers over the Internet. *SYN* refers to the type of message (Synchronize) that is used between computers when a network connection is being made. In this attack, the attacker runs a program from a remote location (anywhere in the world) that jams the service on the victim computer. This is one type of *denial-of-service attack* because the effect of the attack is to prevent a computer from providing its services. The attack might prevent one site from being able to exchange data with other sites or prevent the site from using the Internet at all. Increasingly, companies are depending on Internet services for day-to-day business, from email to advertising to online product delivery. Some companies' business is entirely dependent on the Internet.

SYN attacks have been used successfully against a wide variety of targets, but they have the greatest impact against Internet service providers (ISPs), which provide Internet connection services to government, businesses, and individuals. A SYN attack against an ISP usually results in disruption of Internet service to all the service provider's customers.

This type of attack is very difficult to prevent because it exploits a design flaw in the basic technology used for Internet communication today. Experts are working on techniques to reduce the problem somewhat, but preventing these attacks from occurring in the future will require a change in the way Internet communications are accomplished. This is likely to take several years.

IP Spoofing: Masquerading

In an attack known as *IP spoofing*, attackers run a software tool that creates Internet messages that appear to come, not from the intruder's actual location, but from a computer trusted by the victim. *IP*, which stands for Internet Protocol, refers to the unique address of a computer. When two computers trust each other, they allow access to sensitive information that is not generally available to other computer systems. The attacker takes advantage of this trust by masquerading as the trusted computer to gain access to sensitive areas or take control of the victim computer by running “privileged” programs. Information that has been compromised through IP spoofing includes credit card information from a major Internet service provider and exploitation scripts that a legitimate user had on hand for a security analysis.

Unfortunately, there are many computer programs and services that rely on other computers to “speak the truth” about their address and have no other mechanism for disallowing access to sensitive information and programs. The CERT Coordination Center has received many reports of attacks in which intruders (even novice intruders) used this technique to gain access to computer systems with the help of publicly available IP spoofing computer programs.

Sniffers: Violating Privacy and Confidentiality

For most users of computer networks, including the Internet, the expectation is that once a

message is sent to another computer or address, it will be protected in much the same way letters are protected in the U.S. Postal Service. Unfortunately, this is not the case. Messages sent over the Internet are treated more like postcards sent by a very fast, efficient pony express. Information (such as electronic mail, requests for connections to other systems, and other data) is sent from one computer to another in a form easily readable by anyone connected to a part of the network joining the two systems together. For Internet data, these messages are routed through the networks at many locations, any one of which could be used to read and store the data as it goes by. The CERT/CC has handled many incidents in which an intruder ran a program known as a *sniffer* at a junction point of the Internet.

The sniffer program records many kinds of information for later retrieval by the intruder. Of specific interest to most intruders is the user name and password information used in requests to connect to remote computers. With this information, an intruder can attack a computer on the Internet using the name and password of an unsuspecting Internet user. Intruders have captured hundreds of thousands of these user name/password combinations from major companies, government sites, and universities all over the world.

To prevent attacks of this type, encryption technology must be used for both the access to other computers around the Internet (cryptographic authentication) and the transmission of data across the Internet (data encryption).

Attractiveness of the Internet to Attackers

Compared with other critical infrastructures, the Internet seems to be a virtual breeding ground for attackers. There is (loosely) organized attack tool development in the intruder community, with only a few months elapsing between "beta" software and active use in attacks. Moreover, intruders take an open-source approach to development. One can draw parallels with open system development: there are many developers and a large, reusable code base.

Intruder tools are becoming increasingly sophisticated as well as increasingly user friendly and widely available. For the first time, intruders are developing techniques to harness the power of hundreds of thousands of vulnerable systems on the Internet. Using what are called distributed-system attack tools, intruders can harness a large number of sites simultaneously, focusing all of them to attack one or more victim hosts or networks. The sophisticated developers of intruder programs package their tools into user-friendly forms and make them widely available. As a result, even unsophisticated intruders can use them.

Unfortunately, Internet attacks in general, and denial-of-service attacks in particular, remain easy to accomplish, hard to trace, and a low risk to the attacker.

Internet Attacks Are Easy

Internet users place unwarranted trust in the network. It is common for sites to be unaware of the amount of trust they actually place in the infrastructure of the Internet and its protocols. Unfortunately, the Internet was originally designed for robustness from attacks or events that were external to the Internet infrastructure, that is, physical attacks against the underlying physical wires and computers that make up the system. The Internet was not designed to withstand internal attacks--attacks by people who are part of the network; and now that the Internet has grown to encompass so many sites, millions of users are effectively inside.

The Internet is primarily based on protocols (rules and conventions) for sharing electronically stored information, and a break-in is not physical as it would be in the case of a power plant, for example. It is one thing to be able to break into a power plant, cause some damage, then escape. But if a power plant were like the Internet, intruders would be able to stay inside the plant undetected for weeks. They would come out at night to wander through the plant, dodging a few guards and browsing through offices for sensitive information. They would hitch a ride on the plant's vehicles to gain access to other plants, cloning themselves if they wished to be in both places at once.

Internet attacks are easy in other ways. It is true that some attacks require technical knowledge--the equivalent to that of a college graduate who majored in computer science--but many successful attacks are carried out by technically unsophisticated intruders. As mentioned earlier, technically competent intruders duplicate and share their programs and information at little cost, thus enabling naive "wannabe" intruders to do the same damage as the experts.

Internet Attacks Are Difficult to Trace

As discussed in the IP spoofing example, attackers can lie about their identity and location on the network. Information on the Internet is transmitted in packets, each containing information about the origin and destination. Again, a packet can be compared to a postcard--senders provide their return address, but they can lie about it. Most of the Internet is designed merely to forward packets one step closer to their destination with no attempt to make a record of their source. There is not even a "postmark" to indicate generally where a packet originated. It requires close cooperation among sites and up-to-date equipment to trace malicious packets during an attack.

Moreover, the Internet is designed to allow packets to flow easily across geographical, administrative, and political boundaries. Consequently, cooperation in tracing a single attack may involve multiple organizations and jurisdictions, most of which are not directly affected by the attack and may have little incentive to invest time and resources in the effort.

This means that it is easy for an adversary to use a foreign site to launch attacks against US systems. The attacker enjoys the added safety of the need for international cooperation in order to trace the attack, compounded by impediments to legal investigations. We have seen US-based attacks on US sites gain this safety by first breaking into one or more non-US sites before coming back to attack the desired target in the US.

Internet Attacks Are Low Risk

Failed attempts to break into physical infrastructures involve a number of federal offenses; such events have a long history of successful prosecutions. This is not the case for Internet intrusions. Because attacks against the Internet typically do not require the attacker to be physically present at the site of the attack, the risk of being identified is reduced. In addition, it is not always clear when certain events should be cause for alarm. For example, what appear to be probes and unsuccessful attacks may actually be the legitimate activity of network managers checking the security of their systems. Even in cases where organizations monitor their systems for illegitimate activity, which occurs in only a small minority of Internet-connected sites, real break-ins often go undetected because it is difficult to identify illegitimate activity. In the case of cross-site scripting, web users trigger malicious code without even knowing they have done so, and web sites can unknowingly pass the code along. Finally, because intruders cross multiple geographical and legal domains, there are difficult legal issues involved in pursuing and

prosecuting them.

Need for New Approaches

Today, we rely heavily on the ability of federal investigators and the Internet community as a whole to react quickly enough to security attacks to ensure that damage is minimized and attacks are quickly defeated. However, it is clear that our reactive solutions are reaching the limits of effectiveness. Though individual response organizations are all working hard to streamline and automate their procedures and are working together to better coordinate activities, a number of factors have combined to limit the effectiveness of reactive solutions.

- The number of vulnerabilities in commercial off-the-shelf software is now so high that it is virtually impossible for any but the best resourced organizations to keep up with the vulnerability fixes.
- The Internet now connects nearly 126,000,000 computers and continues to grow at a rapid pace. At any point in time, there are hundreds of thousands of connected computers that are vulnerable to one form of attack or another.
- Attack technology has advanced to the point where it is easy for attackers to take advantage of vulnerable machines and harness them together to launch high-powered attacks.
- Many attacks are now fully automated and spread at nearly the speed of light across the entire Internet community.
- The attack technology has become increasingly complex and in some cases intentionally stealthy, thus increasing the time it takes to discover and analyze the attack mechanisms in order to produce antidotes.
- Internet users are increasingly dependent on the Internet and use it for many critical applications as well as online business transactions; even relatively short interruptions in service cause significant economic loss and can jeopardize critical services.

These factors, taken together, indicate that we can expect many attacks to cause significant economic losses and service disruptions within even the best response times. Aggressive, coordinated response will continue to be necessary, but we must also move quickly to put other solutions in place.

Recommended Actions

We believe the law enforcement community is well positioned to take the lead in developing new methods and infrastructures to deal with the ever-increasing problem of cyber crime. Given the magnitude of the problem today and the problems we are likely to see in the future, we believe that the following actions should be taken:

- Develop a cyber security analysis capability that characterizes the current threat environment in a way that supports system managers in making day-to-day operational decisions to improve security. The analysis methodology should include a predictive capability that anticipates new attacks and allows for pre-emptive action.
- Develop regional activities that bring together a variety of personnel--university; federal laboratory; federal, state, and local law enforcement; and industry--to promote better understanding of both cyber crime prevention and cyber crime investigation techniques.
- Develop scholarship and fellowship programs that develop cyber crime prevention and investigation skills.

Predictive Analysis

Today, there is limited ability to analyze networks and predict threats. Risk analysis is limited by the mistaken assumption that threat changes slowly--that there is time to recognize new vulnerabilities and new intruders and incorporate this new information into comprehensive threat assessments. In many cases, today's threat assessments also are self-limiting because of a lack of understanding of the driving factors behind security incidents in networks.

We need to overcome these obstacles in order to produce accurate and timely warnings of the need for network security efforts. A fused analysis of technical, social, economic, and political triggers is needed. The goal of this analysis should be to identify the need for specific proactive and reactive actions, to provide support for choices among alternative courses of action, and to give insights into the effectiveness of the chosen alternative.

The basic analysis activities include developing an understanding of the normal flow of security-relevant network activity and isolating from that flow the key network behavior patterns that indicate pre-emptive action is needed. The results are well-understood and defensible alerts, with information that supports actions taken to respond to the alert (that is, what to do, how to do it, and when to do it). These are among the factors that must be considered:

- **Time:** Faster methods of intrusion increase the danger to networked computers because they leave less time for response. Time-of-day factors have been used to help to locate perpetrators. Intrusions that happen on specific dates may warrant further investigation, although there have been cases where too much significance has been attached to the date of an intrusion.
- **Source and victim:** Intrusions that originate from an unusual network or computer may warrant attention. Examples are networks known to be especially diligent about security and those associated with specific foreign agencies. (Care must be taken here, as intruders frequently obfuscate the true source of an intrusion as much as possible, by using chains of intermediate computers and by using dial-up networks instead of Internet connections.) Intrusions that affect a sensitive victim also warrant further investigation. Examples are critical infrastructure intrusions that do not follow known methods and intrusions that occur despite careful protective measures.
- **Growth of incidents related to a specific rationale:** The rationale for an incident might be explicitly provided in statements made in web defacements or information left on compromised servers. Certain intrusion tools (such as the May Day tool used in the incidents at the World Trade Organization) place short statements in log files. The rationale might also be suggested by attacks on a cluster of related targets, such as a specific industry or organization, or a tie between an incident and a significant event for an organization.
- **Perpetrators:** Information about perpetrators of incidents is among the hardest information to obtain because perpetrators often hide behind pseudonyms or forged identities. It is somewhat difficult to classify the perpetrators, either in terms of observed characteristics of their level of organization or in terms of the types of intrusions they tend to use. Characterization of intruders as professional, serious threats, or casual hobbyists can aid in identifying incidents of specific interest.

Analysts need to weigh all these factors (technical characteristics, time, source/victim, rationale, and perpetrators), to identify which behaviors are exceptional and which exceptional behaviors prompt warnings. The results of analysis should directly support decision making by the system operator.

The decision support role for predictive analysis involves a) understanding the various courses of action available in response to an alert along with their consequences, b) matching the threat to possible defensive actions, and c) providing those courses of action in a strategic context to decision makers. At the CERT Analysis Center, we believe that separate groups of analysts need to provide this strategic view, as the system and network administrators and incident handlers are often too involved with the tactics of defense to examine objectively their strategic options.

As a course of action is determined and implemented, predictive analysis for networks must begin to take on a new role. Assessing the effectiveness of a given course of action is a multi-purpose effort needed to support and enhance future assessments, to help establish the viability of courses of action and fine-tune them to be more effective, and to examine the nature of the ever-changing threat environment.

To assess this effectiveness, analysts need to formulate criteria for a successful defensive action, collect observations to confirm or deny these hypotheses, and test the hypotheses against the observations. On the Internet, the best method for doing any of these is still an open question. Support for this critical work is essential.

In summary, predictive analysis for networks is a dynamic process. The continuing evolution of technologies would, in and of itself, require constant adjustment of the analysis process. But the situation is far more complicated than that. The Internet is fast becoming a transparent part of the social fabric. Therefore, the impact of network intrusions has effects beyond the simple technical problem of closing off a vulnerability or enhancing perimeter defenses. Analysts must take these factors into account throughout the analysis cycle.

As limited as it is, experience with examining malicious behavior against networked computers shows that constant re-evaluation of the risks and threats is the order of the day. Change is the one constant with regard to the Internet that also affects the analysis cycle. When the effectiveness of an intrusion is determined, it often results in the recognition of a new threat or risk. This, in turn, means that the entire cycle begins again. More information must be collected, sorted, stored, and analyzed, and assessments must be made. And not only are the threats changing, but the potential impact of those threats is evolving as well.

Regional Cyber Forensics and Training Alliances

Cyber security has proven to be a complex, multi-faceted and ever changing problem. The continued rapid advance of information technology, broad, affordable access to the technology, and the increased use of the technology for more sensitive applications in government and industry guarantees that new vulnerabilities and new threats will continue to evolve at a rapid pace. While centralized data collection and analysis capabilities will help build understanding of the overall problem and how it is evolving, it is important to remember that cyber crime prevention and investigation are local activities that require local expertise and local action. In addition, our experience clearly demonstrates that cyber crime is a sensitive topic for most organizations and that they are unlikely to report cyber crimes unless they trust the organization they are reporting to and believe they will get value from the reporting. Also, it is clear that state and local law enforcement organizations are increasingly being called upon to deal with cyber crime problems and that they are seriously lacking in both the skills and facilities to deal with the problem effectively.

To improve the ability of the first-line defenders (local, state, and federal law enforcement personnel and system operators in government, academia, and industry) to prevent cyber crimes

and to build the levels of trust that are needed to encourage incident reporting and investigation, we recommend the development of regional cyber forensics and training alliances (RCFTAs).

Each RCFTA would be focused on building partnerships between

- Universities and federal labs in the region with expertise in cyber security and forensics
- Local, state, and federal investigators and prosecutors from the region
- System operators from regional universities, government organizations, and corporations

Each RCFTA would

- Build, operate, and maintain laboratory facilities that support research into cyber forensics techniques as well as cyber crime investigations
- Provide a laboratory environment where system operators could test proposed security solutions and receive expert technical feedback on the strength of their solutions
- Develop and deliver cyber forensics training programs that allow investigators and system operators from the region to stay abreast of the new forensics methods and tools that are required because of the constantly changing technology and threats
- Conduct cyber security and cyber forensics seminars and workshops that bring together system operators and investigators to discuss timely topics of interest and to build needed trust relationships

We believe this combination of activities would cost-effectively bring together the best talent available in a geographic area, build a regional focal point and shared facility for forensics work, provide affordable training for both law enforcement personnel and system operators, and create an infrastructure that supports the building of trust relationships between the law enforcement community and the private sector.

Scholarships and Fellowships

As outlined in this testimony, the problem of cyber crime is sure to be an ever-changing problem. Those who deal with the problem face a steep and never-ending learning curve to stay abreast of the changing vulnerabilities and threats as well as to maintain an in-depth understanding of the underlying information technology. Investigators and prosecutors need specialized skill sets, but there are few degree programs or refresher programs available to them.

In the past two years, the federal government has initiated a cyber security scholarship for service program that provides scholarships for students taking cyber security degree programs in return for the student's promise to work for the federal government for a period of time. While it is still a young program, the benefits are already being seen. A large number of highly qualified students are applying for entry. In addition, universities have been motivated to create security programs or to expand existing programs with security topics.

We encourage the federal government to institute a similar program in cyber forensics to meet the growing need for skilled investigators and prosecutors. Beginning with funding to support curriculum development, the program should be expanded over time to include scholarships for undergraduate and graduate programs as well as capacity-building programs to encourage new faculty to enter the field.

In addition, to help current law enforcement personnel stay current with the changing

technology, vulnerabilities, and threats, we encourage the development of a fellowship program that allows federal employees to spend a year at a cyber security university center of excellence or cyber security program at a federal lab or research center. The fellow should be given the opportunity to work on research projects that are pushing the state of the art as well as given time to transition the knowledge gained back to his or her parent organization.

Conclusion

The cyber crime problem is an ever-changing and rapidly growing problem. New vulnerabilities and threats are seen regularly, and the damage from attacks has increased dramatically over the past several years. Rapidly evolving attack technology has now reached the point where significant damage can be done within even the best response cycle that can be imagined. Dealing effectively with the problem will require work in a number of areas. The law enforcement community (federal, state, and local) is well positioned to lead in some of these areas, but new techniques and relationships are needed. Emphasis must be placed on building predictive analysis capabilities that give advanced warnings of likely threats with enough detail that system operators can take action to better protect their systems. More attention must be paid to building understanding and capability at the local level. Innovative solutions are needed to leverage existing capabilities at universities and government funded labs and research centers and to build regional centers of excellence that are available and valuable to both government and the private sector. There is currently a shortage of personnel with the knowledge, skills, and abilities to deal with cyber crime. Scholarship and capacity-building programs will help fill this void as well as build a foundation for the research that will be needed to deal with the problems we are sure to see tomorrow.

Meet the CERT® Coordination Center

Overview

The CERT Coordination Center (CERT/CC) is located at the Software Engineering Institute (SEI), a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. Following the Morris worm incident, which brought 10 percent of Internet systems to a halt in November 1988, the Defense Advanced Research Projects Agency (DARPA) charged the SEI with setting up a center to coordinate communication among experts during security emergencies and to help prevent future incidents. Since then, the CERT/CC has helped to establish other response teams, and our incident handling practices have been adapted by more than 90 response teams around the world.

While we continue to respond to security incidents and analyze product vulnerabilities, our role has expanded over the years. Each year, commerce, government, and individuals grow increasingly dependent on networked systems. Along with the rapid increase in the size of the Internet and its use for critical functions, there have been progressive changes in intruder techniques, increased amounts of damage, increased difficulty of detecting an attack, and increased difficulty of catching the attackers. To better manage these changes, the CERT/CC is now part of the larger SEI Networked Systems Survivability Program, whose primary goals are to ensure that appropriate technology and systems management practices are used to resist attacks on networked systems and to limit damage and ensure continuity of critical services in spite of successful attacks ("survivability").

To accomplish our goals, we focus our efforts on the following areas of work: survivable enterprise management, survivable network technology, incident handling, incident and vulnerability analysis, and courses and seminars.

We are also committed to increasing awareness of security issues and helping organizations improve the security of their systems. Therefore, we disseminate information through many channels.

[--Back to top--](#)

Areas of Work

Survivable Enterprise Management

Our survivable enterprise management effort focuses on publishing security practices and developing a self-directed method for organizations to improve the security of their network computing systems.

CERT security practices provide concrete, practical guidance that helps organizations improve the security of their networked computer systems. These practices address the most pervasive problems, as reported to the CERT/CC, and they are technology-neutral for broad application. A complete list of the practices can be found on the CERT/CC web site at <http://www.cert.org/security-improvement/>

The CERT security practices have also been compiled into *The CERT® Guide to System and Network Security Practices*, published by Addison-Wesley. Using a practical, phased approach, the book shows administrators how to protect systems and networks against malicious and inadvertent compromise based on security incidents reported to the CERT/CC.

The Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVESM) is a self-directed approach that gives organizations a comprehensive, repeatable technique for identifying risk in their networked systems and keeping up with changes over time. The method takes into consideration assets, threats, and vulnerabilities (both organizationally and technologically) so that the organization gains a comprehensive view of the state of its systems' security. Details are available from <http://www.cert.org/octave/>

Survivable Network Technology

In the area of survivable network technology, we are concentrating on the technical basis for identifying and preventing security flaws and for preserving essential services if a system is penetrated and compromised. Approaches that are effective at securing bounded systems (systems that are controlled by one administrative structure) are not effective at securing unbounded systems such as the Internet. Therefore, new approaches to system security must be developed. They include design and implementation strategies, recovery tactics, strategies to resist attacks, survivability trade-off analysis, and the development of security architectures. Current work includes the development of our Survivable Systems Analysis method and Easel, a simulation language and tool. This work draws on the vast collection of incident data collected by the CERT/CC. For introductory information, technical reports, and more details, see <http://www.cert.org/research/>

Incident Handling and Analysis

We continue to provide advice to computer system administrators in the Internet community who report security problems. In addition, one of our primary objectives is to analyze the state of Internet security and convey that information to the system administrators, network managers, and others in the Internet community through the various channels described in the Information Dissemination section.

Our understanding of current security problems and potential solutions comes from analysis of security incidents, intrusion techniques, configuration problems, and software vulnerabilities. Contributing to our broad view of the state of security is the information reported to us. Since our inception in 1988, we have received more than 437,500 email messages and more than 20,280 hotline calls reporting computer security incidents or requesting information. We have handled more than 100,300 computer security incidents and received more than 5,000 vulnerability reports. Organizations trust us with sensitive information about security compromises and network vulnerabilities because we have proven our ability to keep their identities and other sensitive information confidential.

The scale of emerging networks and the diversity of user communities make it impractical for a single organization to provide universal support for addressing computer security issues. Therefore, the CERT/CC staff regularly works with sites to help them form computer security incident response teams (CSIRTs) and provides guidance and training to both new and existing teams. For more information about this work, see <http://www.cert.org/csirts/>

Work is under way on AirCERT, an open-source infrastructure for automatically collecting information on security events at Internet sites and automatically handling well-understood attacks. More information about AirCERT is available at <http://www.cert.org/kb/aircert>

Vulnerability Analysis

The CERT/CC has become a major reporting center for both incidents and vulnerabilities because we have an established reputation for discretion and objectivity. Our connection with the Software Engineering Institute and Carnegie Mellon University contributes to our ability to be neutral, enabling us to work with commercial competitors and government agencies without bias.

When we receive a vulnerability report, our vulnerability experts analyze the potential vulnerability and work with technology producers to inform them of security deficiencies in their products and to facilitate and track their response to these problems. Another source of vulnerability information comes from incident analysis. Repeated incidents of the same type often point to the existence of a vulnerability and, often, the existence of public information or automated tools for exploiting the vulnerability.

The CERT/CC makes vulnerability information widely available through a Vulnerability Database: <http://kb.cert.org/vuls/>.

Education and Training

We offer public training courses for technical staff and managers of computer security incident response teams as well as for system administrators and other technical personnel interested in learning more about network security. In addition, several CERT/CC staff members teach courses in the Information Security Management specialization of the Master of Information Systems Management program in the H. J. Heinz III School of Public Policy and Management at Carnegie Mellon University. For more information, see <http://www.cert.org/training/>

[--Back to top.--](#)

Information Dissemination

To increase awareness of security issues and help organizations improve the security of their systems, we collect and disseminate information through multiple channels:

- telephone and email
hotline: (412) 268-7090
email: cert@cert.org
mailing list: majordomo@cert.org
- USENET newsgroup: [comp.security.announce](http://www.cert.org/)
- World Wide Web: <http://www.cert.org/>
- CERT/CC Knowledgebase (the Vulnerability Database is publicly accessible):
<http://kb.cert.org/vuls/>

In addition, headlines about recently published alerts, incident notes, and vulnerability notes are available through an [RSS channel](#).

In addition to responding to more than 20,280 hotline calls and 437,500 email messages, we have published 781 security alerts (advisories, incident notes, vulnerability notes, CERT summaries, and other bulletins).

Publications

Advisories - CERT/CC advisories address Internet security problems. They offer an explanation of the problem, information that helps you determine if your site has the problem, fixes or workarounds, and vendor information. Among the criteria for developing an advisory are the urgency of the problem, potential impact of intruder exploitation, and the existence of a software patch or workaround. On the day of release, we send advisories to a mailing list, post them to the USENET newsgroup [comp.security.announce](http://www.cert.org/) and make them available on the CERT web site at <http://www.cert.org/advisories/>.

CERT summaries - We publish the CERT summary as part of our ongoing efforts to disseminate timely information about Internet security issues. The summary is typically published four to six

times a year. The primary purpose of the summary is to call attention to the types of attacks currently being reported to the CERT/CC. Each summary includes pointers to advisories or other publications that explain how to deal with the attacks. Summaries are distributed in the same way as advisories.

Incident notes and vulnerability notes - We publish two web documents, incident notes and vulnerability notes, as an informal means for giving the Internet community timely information relating to the security of its sites. Incident notes describe current intruder activities that have been reported to the CERT/CC incident response team. Vulnerability notes describe weaknesses in Internet-related systems that could be exploited but that do not meet the criteria for advisories.

Security practices - Security practices provide concrete, practical guidance that will help organizations improve the security of their network computer systems. The practices are available on the CERT web site at <http://www.cert.org/security-improvement/>.

Other security information - We capture lessons learned from incident handling and vulnerability analysis and make them available to users of the Internet through a web site archive of security information and products. These include answers to frequently asked questions, a security checklist, "tech tips" for system administrators, research and technical reports, and a handbook for new computer security incident response teams.

[--Back to top--](#)

Advocacy and Other Interactions with the Community

The CERT/CC has the opportunity to advocate high-level changes that improve Internet security and network survivability. Additionally, CERT/CC staff members are invited to give presentations at conferences, workshops, and meetings. These activities enhance the understanding of Internet security and related issues.

Forum of Incident Response and Security Teams (FIRST) - FIRST is a coalition of individual response teams around the world. Each response team builds trust within its constituent community by establishing contacts and working relationships with members of that community. These relationships enable response teams to be sensitive to the distinct needs, technologies, and policies of their constituents. FIRST members collaborate on incidents that cross boundaries, and they cross-post alerts and advisories on problems relevant to their constituents.

The CERT/CC was a founding member of FIRST, and staff members continue to be active participants in FIRST. A current list of FIRST members is available from <http://www.first.org/team-info/>. More than 110 teams belonged to FIRST, and membership applications for additional teams are pending.

Vendor Relations

We work closely with technology producers to inform them of security deficiencies in their products and to facilitate and track their response to these problems. Staff members have worked to influence the vendors to improve the basic, as shipped, security within their products and to include security topics in their standard customer training courses. We interact with more than 100 vendors, as well as developers of freely available software.

Vendors often provide information to the CERT/CC for inclusion in advisories.

External Events

CERT/CC staff members are regularly invited to give presentations at conferences, workshops, and meetings. We have found this to be an excellent way to help attendees learn more in the area of network information system security and incident response.

Infrastructure Protection

In its incident and vulnerability handling activities, the CERT/CC assigns a higher priority to attacks and vulnerabilities that directly affect the Internet infrastructure (for example, network service providers, Internet service providers, and domain name servers and routers). In addition, CERT/CC staff participates in meetings related to the security of the information infrastructure. One example is meetings of the National Security Telecommunications Advisory Committee's Network Security Information Exchange (NSTAC NSIE) group, which works to reduce vulnerabilities in critical infrastructures.

Media Relations

The CERT/CC works with the news media to raise the awareness of a broad population to the risks they face on the Internet and steps they can take to protect themselves. Ultimately, the increased visibility of security issues may lead consumers to demand increased security in the computer systems and network services they buy.

In the course of a year, the CERT/CC is referred to in major U.S. newspapers and in a variety of other publications, from the *Chronicle of Higher Education* to *IEEE Computer*. Our staff gives interviews to a selected number of reporters, under the guidance of the SEI public affairs manager.

In 2001, the CERT/CC was covered in radio, television, print, and online media around the world, including *Inside Healthcare Computing*, *Information Security*, *Internet World*, *American Banker*, *Wall Street Journal*, *Computerworld*, *IAnewsletter*, *The Washington Post*, *USA Today*, *Security Management*, *US News and World Report*, *Business Week*, *Government Technology*, MSNBC, BBC London, National Public Radio, ABC, CBS, and more. Topics were also picked up by the Associated Press.

[--Back to top--](#)

Appendix A: The CERT/CC Charter

The CERT/CC is chartered to work with the Internet community in detecting and resolving computer security incidents, as well as taking steps to prevent future incidents. In particular, our mission is to

- Provide a reliable, trusted, 24-hour, single point of contact for emergencies.
- Facilitate communication among experts working to solve security problems.
- Serve as a central point for identifying and correcting vulnerabilities in computer systems.
- Maintain close ties with research activities and conduct research to improve the security of existing systems.
- Initiate proactive measures to increase awareness and understanding of information security and computer security issues throughout the community of network users and service providers.

[--Back to top--](#)

Appendix B: The CERT/CC and the Internet Community

The CERT/CC operates in an environment in which intruders form groups and develop scripts that they share with each other on how to maliciously exploit vulnerabilities in systems. Intruders dedicate time to developing programs that exploit vulnerabilities and to sharing information. They have their own publications, and they regularly hold conferences that deal specifically with tools and techniques for defeating security measures in networked computer systems.

In contrast, the legitimate, often overworked, system administrators on the network often find it difficult to take the time and energy from their normal activities to stay current with security and vulnerability information, much less design patches, workarounds (mitigation techniques), tools, policies, and procedures to protect the computer systems they administer.

In helping the legitimate Internet community work together, we face policy and management issues that are perhaps even more difficult than the technical issues. For example, one challenge we routinely face concerns the dissemination of information about security vulnerabilities. Our experience suggests that the best way to help members of the network community to improve the security of their systems is to work with a group of technology producers and vendors to develop workarounds and repairs for security vulnerabilities disclosed to the CERT/CC. To this end, in the absence of a major threat, we do delay disclosing vulnerabilities to give vendors an opportunity to develop a solution. Our [vulnerability disclosure policy](#) contains details and an FAQ.

CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office. Copyright 2002 Carnegie Mellon University.

[Disclaimers and copyright information](#)

Last updated February 5, 2002

CERT® Analysis Center

As technology advances, becoming more complex and integrated into every facet of everyday life, threats to information systems grow at an equal or greater pace. It is this realization that motivated the Network Systems Survivability (NSS) Program of the Software Engineering Institute (SEI) at Carnegie Mellon University to establish the CERT Analysis Center.

The SEI recognizes that information systems are tools that facilitate the accomplishment of an organization's goals and missions. Ensuring that those goals and missions can be met, even if the information systems are under attack, is the primary focus of the NSS Program. Improving network survivability has been a long-standing goal of the SEI, but the primary focus has been technological analysis of threats and a review of penetrations and intrusions of various information systems. In the Analysis Center, the ultimate goal is to provide predictive analysis of possible malicious activity on the Internet.

The CERT Analysis Center was initiated to approach the network survivability problem from a different perspective. Analysts examine not only the technical aspects of the threat environment, but they also take into account the political, economic, and social aspects. To accomplish this effort, the SEI has brought together a cadre of experts with diverse backgrounds. In addition to outstanding information technology and computer professionals, the center also includes experts in the fields of intelligence, organized crime, business, and legal research. In the near future, experts in other the fields, such as insurance and finance, will join the staff. This diversified team focuses on both how system attacks occur and *why*. New predictive analysis methodologies are being developed along with methods for analyzing vulnerabilities, malicious code, and victim and perpetrator profiles. The Analysis Center also works closely with other groups at the SEI for threat modeling and simulation.

The Analysis Center is currently working in support of U.S. Government customers as well as participating in internal research and development efforts. In addition to ongoing work for the government, the Analysis Center also expects to find its niche within the corporate, medical, and academic communities.

Ensuring the survivability of systems operating over the Internet is, and will continue to be, a significant challenge. The analytic and technical experts at the Analysis Center recognize the ongoing nature of the challenge before them and find it an invigorating environment in which to work. Until now, the intruders have always been at least one step ahead of security efforts. It is the goal of the Analysis Center team, with assistance from other SEI experts, to change the state of the intrusion game. A proactive, predictive capability will go a long way toward taking away the advantage currently enjoyed by those whose aims are to cause disruption and chaos on the Internet.



News Release

FOR IMMEDIATE RELEASE

Tuesday, February 26, 2002

FOR ADDITIONAL INFORMATION:

Diane Smirolto, 202-530-5136, dianes@bsa.org

Doug McGinn, 202-715-1558, doug.mcgin@ditlus.com

BSA Applauds Chairman Smith's Leadership in Securing Subcommittee Passage of the Cyber Security Enhancement Act

Washington, D.C (February 26) – The Business Software Alliance (BSA) today commended the House Judiciary Subcommittee on Crime for its swift passage of the Cyber Security Enhancement Act (H.R. 3482), a bill aimed at strengthening federal laws against computer crimes and cyber attacks. In particular, BSA applauded the leadership of Chairman Lamar Smith (R-TX) in spearheading efforts that led to the subcommittee's successful, bipartisan passage of this important legislation.

"The threat of cyber attacks is real, and its fallout is a significant economic drag on the U.S. economy, precisely at a time when we can least afford it. It can expose sensitive government and consumer data and place all Americans at risk," said BSA Vice President of Policy Robert Cresanti. "If we are to protect American consumers, businesses, and government, federal laws against cyber crime must be strengthened. The Cyber Security Enhancement Act will provide law enforcement with needed digital age tools and impose tougher sentencing on those who would threaten our security. BSA commends the efforts of the subcommittee and the leadership of Chairman Lamar Smith in bringing this important legislation a step closer to becoming law."

BSA member company CEOs specifically identified the need to strengthen criminal penalties and civil damages against computer crimes as a key component of enhancing America's cyber security defenses. The CEOs' recommendations are included in a recently released paper, "Partnering for Cyber Security: A Blueprint for a Secure America," which highlights the need to better equip law enforcement with tools and training to enforce penalties and respond rapidly to violators of cyber security laws. BSA firmly believes that H.R. 3482 will help make a real difference in meeting the nation's homeland security objectives. The BSA Blueprint for a Secure America can be found on the BSA website, www.bsa.org/security.

###

The Business Software Alliance (www.bsa.org) is the foremost organization dedicated to promoting a safe and legal online world. The BSA is the voice of the world's software and internet industry before governments and with consumers in the international marketplace. Its members represent the fastest growing industry in the world. BSA educates computer users on software copyrights; advocates public policy that fosters innovation and expands trade opportunities; and fights software piracy. BSA members include Adobe, Apple Computer, Autodesk, Bentley Systems, Borland, CNC Software/Mastercam, Compaq, Dell, Entrust, IBM, Intel, Intuit, Macromedia, Microsoft, Network Associates, Novell, Sybase, Symantec, and Unigraphics Solutions.

1150 18th Street N.W., Suite 700, Washington, D.C. 20036
TEL 202.872.5500 FAX 202.872.5501 EMAIL: info@bsa.org

